

How Varonis Can Help With Efforts Toward Sarbanes-Oxley Compliance

Overview

This document provides a brief overview of the Sarbanes-Oxley Act, Sections 302 and 404 in particular, and summarizes how Varonis data governance solutions can help organizations achieve compliance with certain portions of the directives outlined within the Sarbanes-Oxley Act of 2002.

Background

The Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, and commonly called “SOX” or “Sarbox”, is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals.

As of 2006, all public companies are required to submit an annual assessment of the effectiveness of their internal financial auditing controls to the U.S. Securities and Exchange Commission (SEC). Additionally, each company's external auditors are required to audit and report on the internal control reports of management, in addition to the company's financial statements.

Who Needs To Comply

The SOX legislation establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. It does not apply to privately held companies, although those considering filing for an initial public offering (IPO) must demonstrate a SOX compliant framework. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

For compliance with Section 404, public companies with a market capitalization over US \$75 million needed to have their financial reporting frameworks operational for their first fiscal year-end report after November 15, 2006, then for all quarterly reports thereafter. For smaller companies, compliance is required for the first fiscal year-end financial report, then for all subsequent quarterly financial reports after July 15, 2006.

What Are the Costs/Risks of Non-Compliance

In addition to potential lawsuits and negative publicity, a corporate officer who does not comply, or submits an inaccurate certification, is subject to a fine up to \$1 million and ten years in prison, even if the faulty submittal is not intentional. In the case where an inaccurate certification is submitted purposely, the potential fines increase to \$5 million and twenty years in prison.

SOX, COSO and COBIT

The SEC identifies the Committed of Sponsoring Organizations (COSO) framework by name as a methodology for achieving compliance. The COSO framework defines five components of internal control, which can help support the requirements as set forth in the Sarbanes-Oxley legislation. These five are as follows:

1. **Risk Assessment.** The processes and technologies used in identifying and understanding the areas of risk affecting the completeness and validity of financial reports and other important and sensitive information with impact to financial reporting.

2. **Control Environment.** This is really the foundation of applying the COSO framework and achieving SOX compliance through it. It comprises the integrity and ethics of an organization end-to-end, management's philosophy and operating style, the way management assigns authority and responsibility, and organizes and develops its people as well as the attention and direction provided by the board of directors.
3. **Control Activities.** This includes the approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.
4. **Monitoring.** Auditing processes and schedules to address the high-risk areas within the IT organization. IT personnel should perform frequent internal audits.
5. **Information and Communication.** IT management demonstrating to company management an understanding of what needs to be done to comply with Sarbanes-Oxley and how to get there.

The IT Governance Institute's Control Objectives of Information and Related Technology (COBIT) is also used by many companies as a framework supporting IT SOX 404 efforts. However, there are certain aspects of COBIT that are outside the boundaries of Sarbanes-Oxley regulation. COBIT currently delineates 4 main objectives mapping to 34 IT processes and 318 detailed controls. Of these, only about 12 of the control processes are directly beneficial to SOX compliance. Further, in the discussion of Varonis' Software applicability and benefit toward SOX compliance, we focus on the two most relevant of the 34 control processes: *Ensuring Systems Security and Managing the Configuration*.

- *Ensure Systems Security* - Controls that provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

- *Manage the Configuration* - Controls that provide reasonable assurance that all components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

How Varonis Helps With Efforts for SOX Compliance

The essence of Section 302 of the Sarbanes-Oxley Act states that the CEO and CFO are directly responsible for the accuracy, documentation and submission of all financial reports as well as the internal control structure to the SEC. Section 404 delineates that annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management's assertion that internal accounting controls are in place, operational and effective.

Organizations – and their IT departments in particular – are challenged to meet the requirements of Sections 302 and 404 for any number of systems, applications and data sources that are involved in the accurate reporting of company finances. Varonis provides a comprehensive system for meeting critical objectives of SOX sections 302 and 404 for unstructured data, that is, the contents of file servers. In particular, Varonis solutions ensure that access and use of sensitive and important financial information residing on file servers is automatically ratcheted down to business need-to-know, and that use of sensitive SOX-governed financial information is continuously monitored so that organizations have accurate and non-repudiable proof of data use and compliant behavior at all times.

Specifically, Varonis has created a suite comprised of two products which, when taken together, furnish a complete framework for managing, securing and reporting on all aspects of unstructured data use. They are: DatAdvantage and DataPrivilege.

Varonis DatAdvantage

The Varonis DatAdvantage software solution aggregates user, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need. Specifically, and in a non-intrusive way, Varonis:

- Protects data by recommending removal of overly permissive access controls
- Restricts unstructured data access to those with a business need for that data
- Tracks and monitors every user's every file touch
- Re-computes access controls to account for changes in roles and file server contents

Varonis DataPrivilege

DataPrivilege makes it possible to transition the responsibility of data entitlement management from IT to business owners without any infrastructure changes or business disruption. DataPrivilege brings together data owners and data users in a forum for communicating, authorizing and activating entitlements.

Varonis DataPrivilege allows you to implement a cohesive data entitlement environment, thereby raising accountability and reducing risk. Upon implementation, DataPrivilege provides:

- Data protection by reducing errors in entitlement management
- Business need-to-know access control by enabling data owners to make the call
- Access approval rationale capture for refinement and improvement
- Policy and workflow enforcement for consistency and greater security

The following table provides a mapping between SOX sections, COBIT controls, and the Varonis product suite.

SOX Compliance with Varonis DatAdvantage and DataPrivilege

Requirement	CobIT Control	Description	Varonis Solution
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <ul style="list-style-type: none"> -Risk assessment -Control activities -Information & communication 	<p><i>Ensure Systems Security</i></p> <ul style="list-style-type: none"> - User access administration - Periodic review - Monitoring - Segregation of duties <p><i>Manage the Configuration</i></p> <ul style="list-style-type: none"> - System configuration maintenance - Application and data storage configuration 	<p>Section 302 & 404 outline that a company's CEO and CFO are directly responsible for the accuracy, documentation and submission of all financial reports as well as the internal control structure to the SEC. In order for an organization to confidently attest to this it must have a clear understanding of where data is stored, who owns it, who is responsible for it (steward) and who is authorized to use it.</p>	<p>Varonis DatAdvantage monitors and stores in a searchable format, all aspects of data use for information stored on file servers and Network Attached Storage (NAS) devices. Varonis provides a detailed record of files server contents and how they are used including: filenames, folders, access privileges to files and folders (i.e. a user's or groups NTFS permissions), data use by username or group name (i.e. create, open, delete, rename), a list of the likely business owners of data. This latter is based on Varonis analysis of legitimate user activity on a given data set.</p>
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <ul style="list-style-type: none"> -Control activities -Information and communication 	<ul style="list-style-type: none"> - <i>Ensure systems security</i> - <i>Manage the Configuration</i> 	<p>SOX requires an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. To accomplish this COBIT recommends security officers report directly to high level management and that the following duties be segregated: data entry, computer operation, network management, system administration, systems development and maintenance, change management, security administration, security audit</p>	<p>Varonis helps meet the objectives of these requirements in a number of ways. 1) Varonis recommends the revocation of permissions to data for those users who do not have a business need to the data – this ensures that user access to data is always warranted and driven by least privilege. 2) Varonis generates reports showing the history of permission revocations and the percentages by which overly permissive access was reduced 3) Varonis DataPrivilege provides a mechanism via a web-based application by which to monitor, administer (allow/deny) all access requests to unstructured data. Requestors, data owners, technical controllers, financial controllers are all united in communication and action through this system. With regard to requests to access unstructured data on file shares, all actions taken and rationale for them are recorded. Further, a workflow is enforced (i.e. requests to financial folders go straight to the business owner). Via these capabilities, entities can demonstrate a historical and sustained enforcement of least privilege access and its effects.</p>
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <ul style="list-style-type: none"> -Control activities -Information and communication 	<ul style="list-style-type: none"> - <i>Ensure systems security</i> - <i>Manage the configuration</i> 	<p>Formal security policies, communication of policies and consistent enforcement of policies are critical to running a secure operation. COBIT recommends organizations develop a "framework policy which establishes the organization's overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems."</p>	<p>Varonis DataPrivilege helps organizations not only define the policies that govern who can access, and who can grant access to unstructured data, but it also enforces the workflow and the desired action to be taken (i.e. allow, deny, allow for a certain time period). This has a two-fold effect on the consistent and broad communication of the access policy: 1) it unites all of the parties responsible including data owners, SOX compliance officers, auditors, data users AND IT around the same set of information and 2) it allows organizations to continually monitor the access framework in order to make changes and optimize both for SOX compliance and for continuous enforcement of warranted access.</p>
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <ul style="list-style-type: none"> -Control activities -Monitoring -Information and communication 	<ul style="list-style-type: none"> - <i>Ensure systems security</i> - <i>Manage the configuration</i> 	<p>SOX requires that organizations be able to provide evidence that they are compliant. This requires an ongoing effort to document and measure compliance continuously.</p>	<p>Varonis provides highly detailed reports including: data use (i.e. every user's every file-touch), user activity on sensitive data, changes including security and permissions changes which affect the access privileges to a given file or folder, a detailed record of permissions revocations including the names of users and the data sets for which permissions were revoked. In fact, because DatAdvantage allows any query or complex query of data use within the application to be saved and generated as a report, the amount and types of information that can be furnished for SOX compliance documentation are nearly infinite.</p>

<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <p>-Control activities</p> <p>-Monitoring</p>	<ul style="list-style-type: none"> - <i>Ensure Systems Security</i> - <i>Manage the Configuration</i> 	<p>Accounting for access (particularly administrative access) to critical systems is an important aspect of SOX compliance. Systems must be configured to capture both administrative and user access, to store the logs for later review and to protect the logs from unauthorized access.</p>	<p>Varonis DatAdvantage maintains a detailed history of all objects managed by the Varonis application including users, user groups and by extension administrative accounts within user directories. At any given time users of DatAdvantage can generate reports that show which administrators changed security settings and access permissions to file servers and their contents. The same level of detail is provided for users of data, showing their access history as well as any changes made to security and access control setting of files and folders. Further, alerts and reports are automatically generated for anomalous or overly rigorous activity on important data sets. All of this ensures that access to data in continuously monitored for appropriate use and that organizations have all of the information they need to conduct forensic analysis and process improvement.</p>
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <p>-Control activities</p> <p>-Monitoring</p> <p>-Information and communication</p>	<ul style="list-style-type: none"> - <i>Ensure Systems Security</i> - <i>Manage the Configuration</i> 	<p>Knowing the state of all critical SOX systems and applications is critical to compliance. Change control allows organizations to demonstrate that their state is understood and under control.</p>	<p>As stated above Varonis maintains detailed activity records for all user objects including administrators within active directory and all data objects within file systems. Reports on changes are automatically generated and sent to those parties who have chosen to subscribe for receiving this information via email, to PDA etc. These reports can be generated and sent at user defined frequencies so that the appropriate parties become aware of changes in access controls in a timely fashion that is commensurate with the organization's communication policies.</p>
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <p>-Control activities</p> <p>-Monitoring</p> <p>-Information and communication</p>	<ul style="list-style-type: none"> - <i>Ensure Systems Security</i> - <i>Manage the Configuration</i> 	<p>SOX requires organizations to control access to critical financial systems and account for all changes both to financial records and to the underlying systems and applications that support them. COBIT requires appropriate strength controls present to prevent unauthorized (and unaccountable) access to data, applications and systems.</p>	<p>Varonis addresses these requirements in two key ways:</p> <ol style="list-style-type: none"> 1) Varonis recommends the revocation of permissions to file share data by explicitly and automatically identifying those persons who have no business need to the data for which they have privilege. Varonis system administrators can "commit" the Varonis recommendations through the application 2) Varonis DataPrivilege shifts accountability for data access control from IT to data business owners (which Varonis DatAdvantage will help identify). By administering access control through this application business owners record their rationale and the right parties stay informed of actions taken on data.
<p>SOX Sections 302 and 404</p> <p>COSO Components</p> <p>-Control activities</p> <p>-Monitoring</p> <p>-Information and communication</p>	<ul style="list-style-type: none"> - <i>Ensure Systems Security</i> - <i>Manage the Configuration</i> 	<p>SOX compliance is a continuous process. Auditors look for integration of compliance processes in day-to-day operations.</p>	<p>Varonis understands that unstructured data is growing at rates of 70% or more annually, making SOX compliance, which is an already expensive and arduous proposition, even harder. Varonis has architected a suite robust and complete enough to account for the highly dynamic nature of managing user to data mappings. Further, the company has developed a programmatic and automated means to ensure that access to data is always warranted based on business need-to-know and that the monitoring of use is continuous and relevant to maintaining compliance.</p>

Sources:

- www.pcaobus.org
- www.coso.org
- www.itgi.org
- www.sec.gov
- www.fdic.gov
- www.law.uc.edu
- www.isaca.org
- www.controlit.org