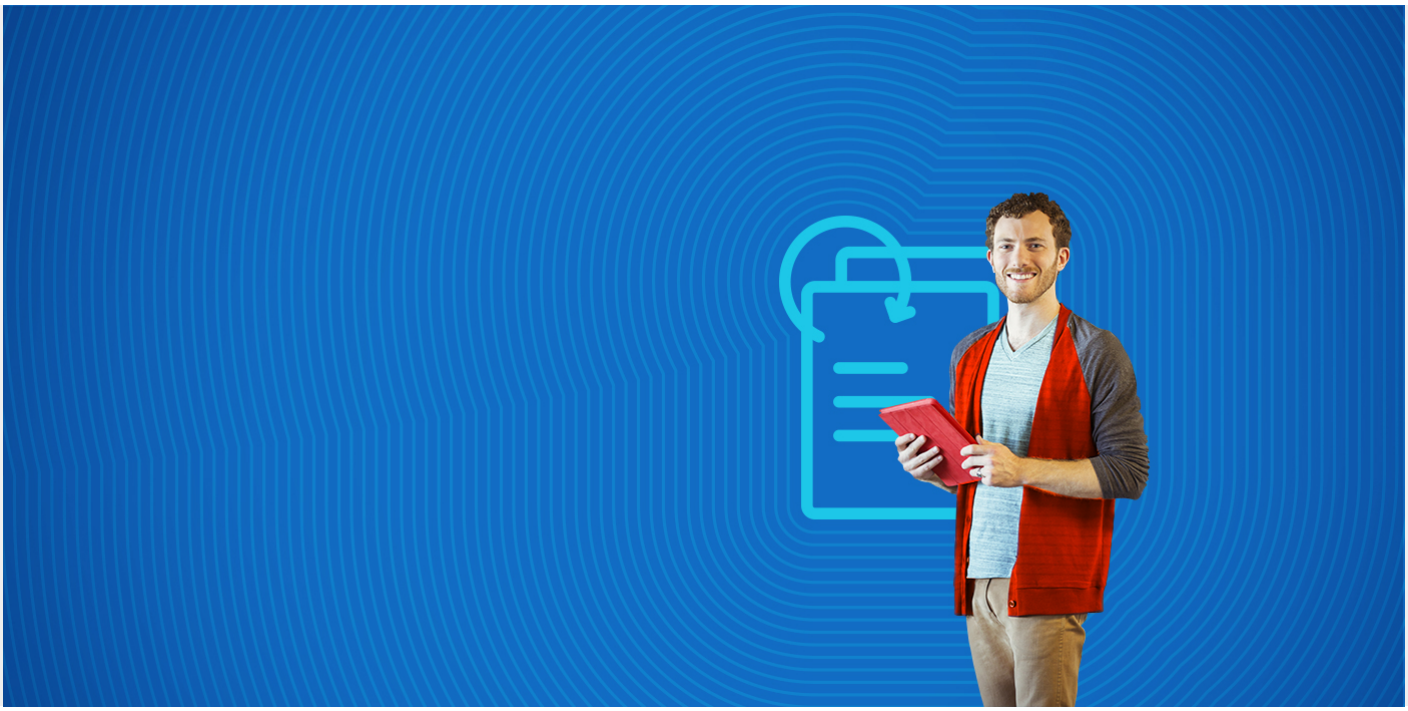
# INTRODUCTION TO SOX COMPLIANCE



## What Is Sarbanes-Oxley (SOX) compliance?

The Public Company Accounting Reform and Investor Protection Act was named after its two sponsors, U.S. Senator Paul Sarbanes and Michael G. Oxley, and it is often referred to as SOX. The act was passed in 2002 in response to major accounting scandals from corporations like Enron and WorldCom, and its goal is to reduce financial malfeasance by increasing penalties for failing to meet accounting standards. In addition to making penalties more severe - they can include millions of dollars in fines and 20 years in prison - the Securities and Exchange Commission also used the act to dramatically increase the standards for accounting records keeping.

Due to the fact that most, and in some cases all, financial records are now digital, SOX compliance requires a particularly robust IT infrastructure. In an effort to ensure that CEOs and senior executives are not given an easy out for producing inaccurate financial reports, lost, mishandled or damaged data is not a valid excuse for noncompliance. Along with averring that data reported is accurate to the best of a person's knowledge, senior management must also state that data was handled and stored in a way that prevented it from being tampered with or lost.

In other words, organizations that are required to meet SOX compliance regulations - which include all publicly traded companies - must have robust IT backup, logging and security systems. Even if a company produces a completely accurate financial report, they still run the risk of getting into legal trouble if weaknesses in their IT infrastructure could have led to the production of a report with incorrect data.

# Legal requirements for IT compliance

SOX mostly deals with financial issues, but sections 302 and Section 404 both include language that relate directly to IT concerns. These sections outline the requirements that the government has for collecting, storing and verifying the accuracy of financial records.

***Section 302***

While there are no specified mechanisms for accomplishing these tasks, Section 302 requires that companies put in place systems that protect against data tampering, provide the ability to track timelines and are able to determine who had access to data and when. Further, companies must be sure that all safeguards are active and that any security breaches or failures to protect data are reported.

***Data Tampering***

Data tampering protections prevent information from being edited by someone who should not have access to financial records or should have read-only access to data. This requires not only that a company protect information from outside interference, such as from malware or a hacker, but that only individuals who should be able to edit data have the right to do so. In addition to using security processes, like firewalls and antimalware software suites, organizations need to ensure that their access controls are managed appropriately. Solutions like BMC BladeLogic Network or Database Automation, a part of the BladeLogic Automation Suite, make automating the audit and management of these controls simple and effective.

A robust access control process will provide the correct levels of access to individuals as well as ensuring that rights are limited or rescinded when appropriate, such as when someone leaves a company or is transferred to a different division. Additionally, businesses must ensure that it is difficult for people to access data without proper credentials. This often means requiring complex passwords, mandatory password changes on a regular basis and appropriate verification of someone's identity before passwords are reset or provided for employees. Further, databases that store login credentials need to be properly encrypted and safeguarded. Many organizations implement audit and remediation of these technical controls using out of the box (OOTB) Compliance Content like that provided with BMC TrueSight Automation for Servers. Regular, automated reports make the effort of sustaining and audit, not to mention passing one significantly less painful.

Another part of preventing data tampering is ensuring that records can be recovered if they are lost, so data backups are key. Financial data needs to be completely recoverable, which ensures that companies always have the most recent and relevant financial records on hand. This is likely to involve multiple and off-site backups, and to be sure of compliance with SOX regulations, it is likely that backups will need to be done far more frequently than many companies are accustomed to. In some cases, a copy of a file may need to be made and stored every time it is changed.

***Timeline Tracking***

Section 302 compliance requires that companies keep track of when changes were made to data. In addition to knowing when a file was last modified, companies may also need to keep a log of when changes are made, what the changes were and who made the changes. Depending on how data is stored and financial entries are managed, it may be easiest for companies to make copies of files every time they are altered and update logs accordingly, which will take care of both redundancy and timeline tracking at the same time.

***Ensuring Safeguards Are Active and Reporting on Their Effectiveness***
Senior management is required to verify the effectiveness and functionality of safeguards and security systems in the 90 days prior to a financial report being made. So long as a system has been installed properly, logs and reports of systems operating effectively are generally sufficient to meet this standard. To ensure that a system is up to the task of protecting data and tracking it, audits will need to be done occasionally. This can be done internally or externally, but it is necessary to provide documentation that audits were completed as well as the findings of the auditors.

Should anything go wrong, either due to outside interference or a problem with systems in place, it is required that this is reported. If a system went down due to a denial of service attack or a malware infection corrupting data, this needs to be included in a report. Even if security breaches or problems were addressed, such as a hard drive failing and data being recovered from a backup, information related to the incidents has to be disclosed.

***Section 404***
This section deals more with transparency than specific objectives related to data handling, and it requires that the efficacy of security systems, protections and data handling methods are independently verifiable. All data must be made available to auditors, including financial records as well as any potential security breaches.

Section 404 requirements are often met by using a remote and web based system that allows access to outsiders. Auditors are given read-only access to files, documents and systems, which allows them to verify that the structures and processes in place are appropriate and sufficient to meet Section 302 requirements.

Since SOX compliance mandates that systems are proven to have been operating as described by regulations for at least 90 days, businesses need to be able to provide reports and logs that indicate system statuses during this time frame. Any security breaches or problems also need to be disclosed along with information about how they were resolved. Most organizations start with incident tracking and monitoring to document these processes and to potentially share with auditors as needed. Organizations that want to get through their audits more quickly and with lower overhead can demonstrate ongoing compliance through meticulous record keeping, or by using an automated Compliance engine like TrueSight Automation for Servers, and the detailed reporting it provides.

## Methods of compliance

It's important to note that there is no one size fits all approach to complying with SOX requirements. Businesses, even those in the same industry, may have vastly different ways of handling their financial documentation and data entry, and organizations may not want to start from scratch with these processes to make them fit a SOX compliant IT process. Additionally, while automating these systems may provide cost savings over the long-term, it may be best for businesses to start handling some tasks manually until it is determined if they are actually effective.

It is important to note that the initial costs of compliance can be high since organizations will need to put systems in place that are able to meet SOX guidelines, train staff to use these new systems and review their effectiveness on a regular basis. As such, most businesses will have to eventually transition to automated systems to keep costs under control.

Generally speaking, the first step for companies who are not yet compliant or want to ensure that

they are compliant is to do an audit. Audits should focus on determining where a system is lacking as well as potential security gaps. Once macro issues have been identified and mitigated, minutiae can be looked at and processes refined. It is common to run quick audits through an organization to assess the compliance posture, and determine where to invest vs. what can remain as-is.

Since getting a company into compliance is likely to involve training people, changes in the current processes, and technology (software and systems) that are being used, it's important that organizations verify that systems work as intended after changes are made. For example, if new accounting software is installed to beef up access control capabilities, it's important to ensure that existing processes are still running correctly.

Complying with SOX does not rule out having a third-party handle IT issues for an organization, but that does not mitigate a business' responsibility to ensure that they are meeting regulations. According to interpretive guidance issued by the SEC, companies are not allowed to issue reports on IT management or data control with limitations; any failures of a third party to comply with standards set out by SOX will still be considered the fault and responsibility of the organization. Therefore, it's important to use a transparent audit process, to have good visibility into the whole compliance picture.

When a company uses a third-party to handle their IT services, they will still need to verify that they are in compliance with SOX regulations. Although this may not be possible in-house, there are still ways to meet the Section 404 requirements for verifying that services are working correctly. Companies have the option of obtaining an assurance report that complies with a Statement on Standards for Attestation Engagements 16 report from the third-party providing their IT services or by having the testing done by an outside consultant.

## COSO and COBIT

There are several existing standards and frameworks in place that may be helpful when designing or updating systems to comply with SOX standards. Two in particular are the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control - Integrated Framework, or COSO, and ISACA's Control Objectives for Information and Related Technology, also referred to as COBIT.

Both COSO and COBIT are frameworks that help organizations determine how to manage and run business processes. They broadly outline the ways that companies can determine what needs to be done to accomplish their goals and how to identify and deal with potential weaknesses. Neither specify the way that IT issues need to be handled; however, this is beneficial since there is no single set way that will work for all businesses.

Using a framework is essential to being able to comply with SOX regulations because the law leaves the method for proving a business' data is safeguarded up to the organization. Therefore, a framework is needed to provide auditors with a way of determining if what is being done to handle data is sufficient to the task and if it is working. Compliance engines like TrueSight Automation for Servers make automating some of these frameworks, and the attendant reporting required achievable with very reasonable Returns on Investment (ROIs), often within 9 months of implementation.

In general, most companies end up using either COBIT on its own or a combination of COSO and COBIT. COSO has the advantage of being a very robust framework for enterprise governance and risk management while being particularly well suited for financial processes, and it has been

endorsed by the SEC.

Still, most organizations do not use COSO on its own is because it falls short in terms of IT planning. However, COBIT fits together nearly perfectly with COSO, and it provides the IT considerations lacking in COSO. COBIT was essentially built upon COSO, but COBIT has fine-tuned COSO so that IT issues are taken into consideration. The two frameworks are so complementary that COBIT documentation refers to COSO components. Other advantages of COBIT are that the framework works well with a number of other established enterprise frameworks, is freely available and has been developed and is still being maintained by a trusted and established non-profit.

COBIT offers a variety of processes and guidelines to help organizations determine what their goals are as well as tracking them. IT control objectives aid businesses in determining what processes need to be put in place based on an organizations particular needs. Once objectives are put in place, they are tracked using the goals and metrics system in COBIT based on IT goals, process goals and activity goals.

In addition to goals and metrics, maturity models show organization where they are in terms of reaching specific objectives. This is a more granular approach to watching an organization's progress, and it can help businesses ensure that they are focusing their efforts on the most important processes as well as making steady progress on achieving their implementation. For help with measuring and improving the maturity of an organization’s technical Audit & Compliance practices, reach out to BMC’s Professional Services organization for expert assistance as a part of their Transform! and Accelerate! Initiatives.

Tested https://bmcmktg.atlassian.net/browse/WEB-11381 on this blog.