S.O.X

In 2002, Congress passed the Sarbanes-Oxley Act (SOX) in response to the fallout and uncertainty following fraud events and financial scandals at several companies, including WorldCom and Enron. The SOX Act introduced several major reforms to the regulation of financial disclosures and corporate governance with the goal of restoring the public's confidence in auditing and financial reporting. The SOX Act, also known as the "Public Company Accounting Reform and Investor Protection Act" or the "Corporate and Auditing Accountability and Responsibility Act," was named after its main architects, Senator Paul Sarbanes and Representative Michael Oxley.

The new or expanded compliance requirements apply to all U.S. public company boards, management, and accounting firms. Private companies contemplating an IPO or gearing up for a merger or acquisition may also find reviewing their SOX internal controls prudent. Among other provisions, SOX mandates:

All companies' financial reports include an Internal Controls report.

Accurate financial data and controls in place to safeguard financial data.

The issuance of year-end financial disclosure reports.

Disclosure of corporate fraud by protecting whistleblower employees.

Kim Pham gives an overview of SOX compliance, impact, challenges and concerns, and leveraging technology solutions for SOX compliance.

Sarbanes-Oxley added accountability requirements for leaders and management, making them liable for the accuracy of their organization's financial statements. Executive misconduct played a major role in the Enron, WorldCom, and Tyco scandals, among others, and continues to influence organizations' attitudes toward financial disclosures and accounting practices. Thus, SOX opened the door for holding executives responsible for fraud in financial reporting. TL; DR SOX compliance ensures companies adhere to rigorous financial reporting standards and internal controls, enhancing transparency and investor confidence. This article covers the essentials of SOX compliance, its implementation, and the benefits it provides beyond mere regulatory adherence.

This article will break down the different SOX compliance requirements, SOX challenges, the benefits of being SOX compliant, and what to expect during the SOX audit process.

Compliance with SOX is enforced by the Securities and Exchange Commission (SEC) As the primary federal agency responsible for protecting investors and maintaining fair and efficient markets, the SEC ensures that companies adhere to the stringent requirements set forth by the Sarbanes-Oxley Act. The SEC's oversight helps to enhance transparency, accountability, and integrity in financial reporting, thereby fostering investor confidence and market stability. The Public Company Accounting Oversight Board (PCAOB) was a new agency established by SOX and is responsible for overseeing the public accounting firm and the quality of their public company audits. The Sarbanes-Oxley Act of 2002 consists of 11 titles, but there are two key provisions regarding compliance requirements: Sections 302 and 404.

Section 302: Corporate Responsibility for Financial Reports

SOX Section 302 states that Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) are directly responsible for the accuracy of financial reports. Signing officers must review and certify the accuracy of financial statements, establish and maintain internal controls, and disclose all significant deficiencies, fraud, and significant changes in internal controls.

This mandate allows CEOs and CFOs to be held accountable for inaccuracies in their organization's financial statements, up to and including criminal penalties. Non-compliance with SOX Section 302 can result in significant civil and criminal penalties, including fines up to $5 million and imprisonment for up to 20 years for executives who knowingly certify false financial reports.

Section 404: Management Assessment of Internal Controls

Section 404 states that all annual reports must include an Internal Control report explicitly outlining management's responsibility to maintain an adequate internal control structure, an assessment of its effectiveness, and any shortcomings in those controls. Independent external auditors must also attest to the accuracy of the company's statement that internal controls are in place and effective. Section 404 includes additional requirements such as a review of a company's internal controls by external auditors and provides exemptions for certain companies. Audit Board's review of SOX 404 offers more detailed information on this SOX section.

To limit conflicts of interest, the external 404 audit must be performed by independent auditors who exercise professional

skepticism and judgment to examine the state of internal controls at publicly traded companies.

The Benefits of SOX 404 Compliance

One of the critical outcomes of Sarbanes Oxley was the end of self-regulation and the establishment of independent oversight of the auditing process through the Public Company Accounting Oversight Board (PCAOB). The PCAOB can establish industry standards, investigate fraud allegations, and regulate audit firms. Indeed, the PCAOB performs regular audits of the auditors to ensure that quality remains high and industry best practices are followed.

As much as companies struggled initially with the cost and resource burden of compliance, over time, they are seeing the investment in SOX compliance pay off in several significant ways.

1. Improved corporate governance: SOX compliance improved corporate governance through the greater regulation of audit committees. Before SOX, 51% of public companies had audit committees completely independent of management. SOX mandated that all listed companies have an audit committee whose members are independent of management and contain at least one financial expert. As a result, audit committees today are better equipped to provide accurate and truthful financial reports. Independent audit committees have a different mandate than others, adding another layer of governance to the financial reporting process.

2. Increased accountability: SOX compliance makes executives more accountable and protects investors. Executives are

required to personally certify financial reports, with significant penalties in place for fraudulent activities. Auditors, too, have a heightened responsibility to maintain integrity and independence as the fraud scandals that fueled Sarbanes-Oxley also led to the downfall of Arthur Andersen, one of the largest accounting firms at the time.

3. Improved auditor independence and quality: SOX compliance enhances auditor independence by prohibiting audit firms from providing bookkeeping, actuarial, or management functions to the companies they audit. External auditors must maintain independence in appearance and in fact. This improves audit quality and the rigor of the audit.

4. Fewer financial restatements: Post-SOX, the number of financial record restatements continues to decline year-over-year, decreasing from 1,784 in 2006 to 738 in 2012.

5. Improved risk management and cybersecurity posture: Many of the best practices implemented by present-day organizations as part of SOX compliance, especially IT General Controls, overlap with guidance from cybersecurity frameworks like the NIST CSF. One example of this overlap is the call for strong, restricted access control and access management to protect sensitive systems and information from unauthorized access — most SOX 404 audits require this for financially material information systems, and the NIST CSF highly recommends this as part of their "Protect" pillar.

To summarize, some of the major benefits of maintaining and iterating on SOX compliance at your organization, other than

simply remaining in compliance are: 1) improved corporate governance, 2) increased accountability, 3) improved auditor independence and quality, 4) fewer financial restatements, and 5) improved risk management and cybersecurity posture.

The Evolution of SOX: Tech Adoption and Cost Focus Amid Business Changes, Cyber, and ESG Mandates

The SOX Audit Process

SOX audits can be broken down into any number of steps, from performing risk assessments to what to include in an audit committee report. We've narrowed our outline of the SOX audit process to the following eight steps:

Defining the Audit Scope Using a Risk Assessment Approach

Determining Materiality and Risks – Accounts, Statements, Locations, Processes, Systems, and Major Transactions

Identifying SOX Controls – IT General Controls (ITGCs), Application Controls, Entity Level Controls (ELCs), etc.

Performing a Fraud Risk Assessment

Managing Process and Control Documentation

Testing Key Controls

Assessing Deficiencies

Delivering Management's Report on Controls

1) Defining the SOX Audit Scope Using a Risk Assessment Approach

For performing a risk assessment, PCAOB Accounting Standard No. 5 states, "A top-down approach begins at the financial

statement level and with the auditor's understanding of the overall risks to internal controls over financial reporting. The auditor then focuses on entity-level controls and works down to significant accounts, disclosures, and their relevant assertions." Boiling this down, the PCAOB recommends that the audit begins at the highest level, becoming more granular. The focus of the audit scope should be those assets, people, systems, and processes that affect the financial disclosure process — which means that not everything in the organization will be in scope. A SOX audit scope should include and consider all risks to an organization's internal controls over financial reporting in a risk-first approach to SOX compliance.

This step in a SOX compliance audit should not result in a list of compliance procedures. Still, it should help the auditor identify potential risks and sources, how it might impact the business, and whether the internal controls will provide reasonable assurance that a material error will be avoided, prevented, or detected.

2) Determining Materiality in SOX – Accounts, Statements, Locations, Processes, and Major Transactions

Step 1 – Determine what is considered material to the P&L and balance sheet. How: Financial statement items are considered "material" if they could influence the economic decisions of users. Auditors can typically determine what is material by calculating a certain percentage of key financial statement accounts. For example, 5% of total assets, 3-5% of operating income, or some analysis of multiple key P&L and BS accounts.

Step 2 – Determine all locations with material account balances. How: Analyze the financials for all the locations you do business

in. If any of the financial statement account balances at these locations exceed what was determined as material (in Step 1), chances are they will be considered material and in-scope for SOX in the coming year. Step 3 – Identify transactions populating material account balances How: Meet with your Controller and the specific process owners to determine the transactions (i.e. debits and credits) that cause the financial statement account to increase or decrease. How these transactions occur and how they're recorded should be documented in a narrative, flowchart, or both.

Step 4 – Identify financial reporting risks for material accounts. How: Seek to understand what could prevent the transaction from being correctly recorded, or the risk event. Then, document the effect the risk event could have on how the account balance could be incorrectly recorded, or the breakdown of the financial statement assertion.

3) Identifying SOX Controls – Key and Non-Key Controls, ITGCs, and Other Entity-Level Controls (ELCs)

During your materiality analysis, auditors will identify and document SOX controls that may prevent or detect transactions from being incorrectly recorded. They will seek to identify the checks and balances in the financial reporting process that ensure the transactions are recorded correctly, and account balances are calculated accurately. Some examples of preventative or detective SOX controls include:

Separating conflicting and incompatible duties (e.g., the ability to post and approve invoices),

Reviews of individual or multiple transactions recorded in the period, and

Account reconciliations.

Next, material accounts often need multiple controls in place to prevent a material misstatement from occurring. You'll have to analyze all the controls to determine which ones best provide assurance, keeping in mind the people, process, and technology in place.

Audit teams are cautioned from applying a brute-force approach and creating a new SOX control whenever a new risk is identified. Inadvertently, each new control is often classified as "key" without performing a true risk assessment, contributing to the ever-increasing control count. By understanding the differences between key and non-key controls, internal audit teams can effectively combat rising control counts and "scope creep."

To keep things simple, the quickest method to differentiate a non-key vs. key control is to refer to the level of risk being addressed. Is the control mitigating a low or high risk? By understanding the risks affecting the SOX compliance process, audit teams can better prioritize and focus their efforts on key controls.

Lastly, to finalize and plan for an effective system of internal controls, your audit team must identify manual and automated controls. For the automated controls identified, you should evaluate whether the underlying system is in-scope for IT General Controls (ITGC) testing, which will impact your overall testing strategy of the control. If you have ITGC comfort over the underlying system, you can substantially reduce the amount of control testing needed to be performed. Operating strong ITGCs

and cybersecurity-related controls are another benefit of SOX compliance.

4) Performing a Fraud Risk Assessment

An effective system for internal controls includes an assessment of possible fraudulent activity. Prevention and early detection are crucial to reducing instances of fraud in an organization. Internal controls play a key role in reducing the opportunities available to commit fraud and what the material impact would be if fraud occurred, including a manual override of internal controls.

Below are examples of anti-fraud internal controls and practices organizations can implement to considerably lower losses due to fraud.

Segregation of Duties: The Institute of Internal Auditors (IIA) describes the basic idea underlying segregation of duties as "no employee or group of employees should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties." That is, the work of one individual should be either independent of, or serves to check on, the work of another. Examples:

Custody of Assets

Authorization/Approval of related transactions affecting those assets

Recording and reporting of related transactions

Expense Reimbursements: As per ACFE's 2014 report, a significant portion of asset misappropriation schemes involve situations in which an employee makes a claim for reimbursement of fictitious or inflated business expenses. To

prevent such schemes, management should ensure the relevant policies and procedures surrounding employee reimbursements are communicated to employees and updated whenever necessary. Moreover, the approval flow for such reimbursements should include, along with the direct supervisor, other key stakeholders, such as affected business team members, payroll, or internal audit.

Whistleblower Hotline: Despite federal regulations, the ultimate responsibility of implementing a strong whistleblower program lies with management. Historically, internal employee tip-offs have provided the best means of fraud detection. Hence, management cannot afford to neglect an internal whistleblower mechanism within the organization.

Periodic Reconciliation of Bank Accounts: Bank reconciliations highlight the differences between the cash per balance sheet and bank statement, while also confirming the accuracy of the data recorded in the organization's cash ledger. The core duty of performing a bank reconciliation is not just to identify unexpected differences but also entails preventing future occurrences, such as accounting delays, restricting auto-debits to vendors, etc. Depending on the size of the organization, bank reconciliations should be performed daily, weekly, or monthly to monitor and detect fraudulent activity.

It is management's proactive approach towards fraud detection and prevention, coupled with strong internal controls, which will ultimately decrease the opportunities to commit fraud and instill an ethical culture within an organization.

5) Managing Process and SOX Controls Documentation

The control narrative and documentation establish details of the operation of key controls, such as control descriptions, frequency, test procedures, associated risk, population, and evidence. Risk and control mapping often has a many-to-many relationship, making manual documentation difficult. Some examples include risks appearing across multiple processes or business units, audit issues impacting multiple controls or processes, and COSO principles mapping to many controls. As an audit manager can attest, if one member of the team fails to make a timely edit or forgot to make updates across all test sheets, the downstream ripple effect can cost managers hours and hours of cleanup. The solution is to leverage an underlying relational database to act as a central repository and as the foundation of the audit program. SOX software constructed upon purpose-built database structures can allow auditors to pull or push information to and from a database quickly and have those results cascade throughout the entire SOX program instantly. Controls documentation is simple and doesn't require making edits across several standalone spreadsheet files. In addition, for annual audit results to be used year over year, a spreadsheet cannot handle large volumes of data. The speed, accuracy, and scalability of a database solution will exceed the benefits of "spreadsheet familiarity."

6) Testing Key Controls

The overall objective of SOX control testing is threefold – 1) ensure the process or test procedures as outlined are an effective method for testing the control, 2) the control is being performed throughout the entire period and by the assigned process owner,

and 3) the control has been successful in preventing or detecting any material misstatements. In short, control testing validates the design and operating effectiveness of controls.

The actual SOX controls testing process may include a variety or combination of testing procedures including ongoing evaluation, observation, inquiries with process owners, walkthrough of the transaction, inspection of the documentation trail, and/or a re-performance of the process.

7) Assessing Deficiencies in SOX

Ongoing investment into a SOX program will naturally result in the improvement of your actions, policies, and procedures. As the control environment improves, businesses will also likely see a clear increase in the level of automation and a corresponding decrease in the amount of manual testing required by auditors. Ultimately, this will lead to your team spending less time managing fewer overall issues. Deficiencies should be reduced to an acceptable and predictable level, and there should be little to no surprises.

During the SOX control testing process and analysis, the auditor may identify an exemption, deficiency, or gap in the tested sample. If this happens, an "issue" is created. Besides remediating and correcting the issue, the audit team then assesses if it was a design failure in the control or an operating failure where training, responsibilities, or process needs to be adjusted. Lastly, management and the audit team assess whether or not it is a material weakness (as described above is typically a percentage of variance and with a high-risk level) and will be reported on the end-of-year financials or if it was only a significant weakness.

8) Delivering Management's Report on Controls

The end product of SOX control testing is management's report on controls over financial reporting being delivered to the audit committee. While a substantial amount of documentation and data is collected during the process, the report should include:

Summary of management's opinion and support for those conclusions.

Review of the framework used, evidence collected, and summary of results.

Results from each of the tests – entity-level, IT, key controls.

Identification of the control failures, gaps, and corresponding root causes.

Assessment made by the company's independent, external auditor.

SOX ITGCs and Security Controls

With the technology landscape evolving rapidly, companies' reliance on information technology and systems for managing financial information significantly affects how a company compiles and delivers its Securities and Exchange Commission (SEC) reports. Since most companies have moved financially significant functions and operations to information systems, including accounting functions, financial functions, and even retail/e-commerce functions, the impact of successful cyberattacks on an organization can be severe. Even without affecting a business' SOX compliance activities, security incidents can lead to data breaches and data loss, creating another set of challenges for a company.

Some of the foundational ITGCs that are tested as part of SOX can help avert security breaches and tampering with financially material information. By establishing effective security controls around data protection, change management, and sensitive data, IT departments can better detect, prevent, and perform remediation for any potential security incidents. Even companies that heavily leverage cloud services and do not have data centers of their own should regularly review their third-party vendors' compliance reports to validate that vendors' standards for data security are in compliance with your organizations. Non-compliance on the part of a vendor can still hold considerable risk for that vendor's customers.

Common SOX Compliance Challenges

Spreadsheet and End-User Issues

The lowly spreadsheet has evolved to be more than just a bookkeeping tool. Over time, the simple spreadsheet has morphed into a SOX workflow staple, due in part to its ability to link data across different documents and automate basic tasks. At the same time, modern audit projects now require more attributes and details about control. Whether it's documenting the completeness and accuracy of evidence, or validating the integrity of a key report, testing procedures have evolved beyond simple attribute ticking and tying. The modern spreadsheet can handle this robust testing process but lacks speed, efficiency, and consistency.

In addition to what's mentioned above, there are certain risks related to using spreadsheets for your SOX program, including, but not limited to:

Miskey by a user or deleted data

Analysis of inconsistent data set — i.e., population is incorrect

Process owners left in the dark

Process owners who own the day-to-day control activities are often left in the dark when it comes to their own controls. Internal Audit teams rely on spreadsheets and shared folders to manage their controls, so documentation often remains on the desktop of internal audit teams — far away from process owners.

When control documentation lives with Internal Audit, process owners only get visibility into their controls once a quarter and thus create their own day-to-day activities driven by their own version of tasks, and not necessarily within the context of their own controls.

Rising Costs and Resources

While SOX has positively impacted financial reporting, concerns remain over the increasing cost of SOX compliance and heavy resource burdens. SOX costs continue to rise year-over-year for many companies, according to Protiviti's annual Sarbanes Oxley Survey. Reasons include the introduction of new frameworks such as COSO and evolving external auditor requirements for Section 404 compliance. Companies today spend an average of one million to two million dollars and up to 10,000 hours on SOX programs annually.

Simplify SOX Compliance with Purpose-Built Technology

One key to decreasing the costly and time-consuming nature of SOX compliance and maximizing SOX resources lies in leveraging purpose-built technology to automate processes. Forward-thinking SOX teams are leveraging SOX automation tools to reduce the administrative hours and efforts spent on SOX. SOX compliance software enables teams to free up time to perform more value-add audits, increase the quality of internal controls, improve real-time visibility into SOX environments, boost external auditor collaboration — and ultimately avoid financial restatements.

Frequently Asked Questions About SOX Compliance

What is the Sarbanes-Oxley Act (SOX) and why was it enacted?

The Sarbanes-Oxley Act, commonly known as SOX, is a U.S. federal law enacted in 2002 to protect investors by improving the accuracy and reliability of corporate disclosures. It was passed in response to major corporate and accounting scandals, including those involving Enron and WorldCom, to restore public confidence in the financial markets.

What are the key requirements of SOX compliance?

SOX compliance requires companies to implement and maintain robust internal controls over financial reporting. Key requirements include the certification of financial statements by CEOs and CFOs (Section 302), the establishment of an internal control framework (Section 404), and the independence of external auditors (Section 301). Companies must also conduct regular SOX audits to ensure compliance with these standards.

How can a company ensure successful SOX compliance?

To ensure successful SOX compliance, companies should establish a dedicated SOX compliance team, implement comprehensive internal controls, and conduct regular training for employees. Utilizing audit management software like Audit Board can streamline compliance processes by automating workflows, providing real-time data analytics, and generating detailed compliance reports. Regular audits and continuous monitoring are also essential to maintain compliance and address any issues promptly.

Vice

Vice Vicente started their career at EY and has spent the past 10 years in the IT compliance, risk management, and cybersecurity space. Vice has served, audited, or consulted for over 120 clients, implementing security and compliance programs and technologies, performing engagements around SOX 404, SOC 1, SOC 2, PCI DSS, and HIPAA, and guiding companies through security and compliance readiness. Connect with Vice on LinkedIn.