FINANCIAL CONTROLS
WHITE PAPER

MITRATECH

FINANCIAL CONTROLS

Mitratech's SOX/SOC-in-a-Box solution to meet Internal Control over Financial Reporting (ICFR) requirements and help your organization ensure SOX and SOC compliance.

Introduction

Major accounting scandals in the past have led to the adoption of the Sarbanes-Oxley Act (SOX) almost 20 years ago..

Section 4 of the act, commonly known as SOX 404, requires the implementation of adequate **Internal Control over Financial Reporting (ICFR)** within listed companies to guarantee fair financial reporting practices in accordance with **Generally Accepted Accounting Principles (GAAP)**. External auditors must attest to the design and effectiveness of the Internal Control over Financial Reporting and the accuracy of their financial statements.

Seeming like a rather fair and straightforward request, SOX requirements have been condemned due to their vague nature and the missing differentiation between key process parts. Being left in the dark, corporations in the early days had to choose between two paths: Either interpret and adopt the new regulations to the best of your capacity, not knowing what best practices are supposed to look like and how the external auditor would interpret their efforts, or over-deliver by creating controls for every process disregarding its significance for financial reporting. The latter approach ultimately developed into the best practice, for a certain period of time, putting tremendous strain on larger corporations in particular.

Given the lack of automation and digitization, manual efforts to comply with the law have been ramped up, resulting in cumbersome print-outs to obtain and reflect proper sign-off, even for the most irrelevant process steps.

Over time, suffering from a bad reputation due to burdensome administration and being far from reflecting business reality, SOX has been amended multiple times. Just recently the SEC relaxed certain requirements for small businesses. However, even after a few large companies underwent delisting procedures, SOX 404 remains a key regulation for companies listed at the New York Stock Exchange, as well as for those aiming to leverage significant fundings and enhance shareholder confidence.

The Evolution of Financial Controls

Since the codification of internal accounting controls nearly four decades ago, the requirements of financial controls and reporting have become more clearly defined:

- The Watergate scandal led to the **Foreign Corrupt Practices Act (FCPA)** in 1977 resulting in Internal accounting controls being codified for the first time.
- The Enron scandal led to the **Sarbanes-Oxley Act (SOX)** in 2002 under the official name: "Public Accounting Reform and Investor Protection Act".

SOX Title IV (Section 404) focuses on internal accounting control rules.

Public companies are required to annually assess the effectiveness of ICFR, disclose the results and engage external auditors.

- **The Committee on Sponsoring Organizations (COSO)** became a guiding principle on how to interpret SOX and its vague requirements and released definitions such as internal controls. (Guidance released in 1992, with an update in 2003).

The COSO model lays out clear principles on how to structure internal control frameworks. According to COSO, there are three types of internal controls:

1. Those that affect a company's operations.
2. Those that affect a company's compliance with laws and regulations.
3. Those that affect a company's financial reporting.

COSO

- Globally accepted framework.
- Covers internal controls as well as Enterprise Risk Management.

ICFR

- One sphere of internal controls.
- Focused on financial integrity.
- Entity Level, Process Level & IT General Controls.

SOX SECTION 4

- U.S. specific.
- Listed companies.

SOX Requirements

SOX applies to all publicly traded companies in the United States as well as wholly-owned subsidiaries and foreign companies that are publicly traded and do business in the United States.

The Internal Controls Report, mandated by Section 4 of the Act, commonly known as SOX 404, requires that all applicable companies have adequate internal controls in place to report accurate financial data in their annual reports. More specifically, SOX 404 requires companies to implement adequate Internal Control over Financial Reporting (ICFR) to ensure fair financial reporting practices have been put in place in accordance with Generally Accepted Accounting Principles (GAAP).

In order to be compliant with SOX, organizations are required to create controls that cover a large scope of IT and financial requirements, all tailored to their unique structure. The design and effectiveness of which will be investigated by the organization's assigned SOX Auditor.

1. Ownership & Responsibility

Section 302 states that the CEO and CFO are directly responsible for the accuracy and submission of all financial reports and internal control structure to the Securities and Exchange Commission (SEC).

2. Management of Internal Controls

Section 404 states that management is responsible for the management of effective internal controls and accurate financial records, reporting on any shortcomings.

3. Data Security Policies and Strategies

Section 404 requires data security policies and strategies to be clearly formalized, communicated and enforced to protect all stored and utilized financial data.

4. Continuous Monitoring and Documenting

It is required that organizations continuously monitor and provide documentation measuring their SOX compliance objectives.

Implementing ICFR to Achieve Reasonable Assurance

Both internal and external audit functions follow this concept when evaluating the effectiveness of internal controls.

Originating in the field of external audit, reasonable assurance asserts that financial statements are free of material misstatements, based on the evidence provided by the client. Internal audit similarly employs this principle to assess an organization's internal control framework in terms of effectively managing associated risks.

The work of auditors is especially important for publicly listed companies and their shareholders, but the ramifications of reasonable assurance can have a far greater impact than it may appear at first glance.

Recent events put the spotlight on major accounting firms and raised questions about how diligently they conduct their day-to-day tasks. An example of this would be the auditing of financial statements of listed corporations.

By default, auditors only verify a certain amount of transactions, including supporting evidence of the transactions in question, that have occurred over a specific period of time. The scope of an audit is constrained by time and budget, as is any other corporate function – this is where reasonable assurance comes into play. Both internal and external audit functions, to a certain extent, have to trust the information provided by their counterparts.

The sheer volume of a company's transactions only allows for a certain degree of scrutiny in reviewing evidence and does not account for an unwarranted investigation of unfounded criminal intent. This limitation of scope is there by design and it holds for all audit engagements where neither criminal intent nor fraud are the focus of consideration.

While it is almost impossible to achieve full assurance on the reliability of financial reporting given the vast amount of data and complexities involved, the goal must be to minimize the risk of misstatements within your financial reporting. One way to achieve this goal is to implement proper Internal Controls over Financial Reporting (ICFR) to guarantee a level of reasonable assurance on your financial integrity.

Reasonable Assurance – A term that speaks to both internal and external audit.

SOX & SOC: Compliance with ICFR

Both SOX and SOC compliance services strive for enhanced financial data accuracy and greater internal control support.

The SOC 1 auditing standard focuses on financial controls related to systems established at service and subservice organizations. By undergoing a SOC 1 assessment, the service organization asserts that proper internal financial controls are put in place and that they are properly designed and functioning as required.

This is key since the client of the service organization must report any outsourced services that might impact its financial records to its shareholders. The responsibility for disclosing accurate financial statements remains with the organization, but their financial controls will be put under scrutiny by the auditors.

For private entities, SOC 1 compliance is said to strengthen both confidence in financial statements and fraud prevention. Despite SOC 1 and SOX being fundamentally different, both focus on compliance with ICFR and highlight the importance of appropriate reporting mechanisms.

Mitratech's GRC Platform Alyne Internal Control over Financial Reporting (ICFR) control set allows for a complete health-check of the financial integrity of an organization, for both SOX and SOC compliance.

SOX

SOX is a government-issued law for enhanced financial information disclosure and the IT security of financial data. Typical users of SOX:

- US publicly-traded companies.
- Wholly-owned subsidiaries of publicly-traded companies.
- Non-US-based, publicly-traded companies who conduct business in the US.
- Private companies preparing to go public with an IPO.

SOC

SOC is an audit of internal controls to ensure data security, suitability of control design and shareholder confidence. Typical users of SOC:

- Data centers.
- Banks and investment firms.
- Healthcare practices.
- Co-Location service providers.
- Tax service providers.
- Any organization that cannot afford a data breach.

How can Mitratech help?

In today's day and age, assurance mechanisms need to be implemented in an efficient way to benefit the organization by:

- Providing the right level of control needed to ensure compliance and financial integrity.
- Seamless interaction and collaborative user engagement within the wider business and the vendor ecosystem.
- A simplified and smart approach to compliance - such as having a single defined requirement and assessment for various reports and interpretations.
- Automatically gathering analytics from assessment responses which help identify risks and provide meaningful guidance.

Conclusion

In Closing

With the ambiguity of SOX requirements and the complexities of financial reporting, technology can be a powerful ally that can help minimize the risk of misstatements within your financial reporting and achieve a level of reasonable assurance on your financial integrity.

Moreover, understanding maturity, having the ability to identify shortcomings, and derive appropriate countermeasures should not only be a goal for those organizations preparing for upcoming audits and certifications, but any organization aiming to go the extra mile in terms of financial integrity and stakeholder confidence.

Industry Expert Opinion Piece

With the 20 year anniversary of Sarbane Oxley upon us it is always good to reflect on its impact and success. Enron showed us the need for standardization in financial controls but at what cost. As outlined in this paper the differences in interpretation have resulted in very different internal control environments being adopted, with some questioning the huge cost of being compliant.

It is unlikely that we will see a relaxing of financial control regulations, for example, as a result of accounting scandals in the UK, a form of "UK SOX" will be announced in 2022/23 which will likely be aimed at not just listed entities but also PIEs (Public Interest Entities).

The UK Government's stated objectives are:

1. Build trust and credibility in the UK's audit, corporate reporting and corporate governance system.

2. Ensure accountability for those playing key roles in said system.

3. Increase resilience and choice in the statutory audit market. The key is, it is hoped, that these reforms will further increase trust in the UK as a place to invest and to obtain investment, which is the objective of all regulatory bodies.

Whether a firm's objective is compliance with these regulations, or best practice, technology can play a huge role in ensuring that a firm can demonstrate to its board of directors, audits and shareholders, as a minimum, that effective controls are in place but also give early insight into emerging risks to ensure early intervention and do so in a cost effective way.

- Henry Umney

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk, and compliance professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise. With Mitratech's proven portfolio of end-to-end solutions, enterprises worldwide are able to implement best practices and standardize processes throughout their organizations and realize fast time-to-value. Serving 1,800 organizations of all sizes worldwide, Mitratech works with almost 40% of the Fortune 500 and over 500,000 users in over 160 countries.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com

© 2022 Mitratech Holdings, Inc. All rights reserved.