Sarbanes-Oxley at 20: For CFOs, it may be time for a refreshing experience

July 30, the twentieth anniversary of the Sarbanes-Oxley Act (SOX), may have gone unnoticed by many US finance executives. But the law is almost certainly present in their day-to-day work lives.

Since it was enacted, SOX has improved transparency and investor confidence in US capital markets. By imposing strict new controls over financial reporting processes, mandating criminal penalties for senior executives who certify false financial statements, and enacting new regulations ensuring auditor independence, Congress accomplished what it set it out do to: end the rash of accounting scandals that plagued financial markets in the early 2000s.[1]

But evolving regulatory requirements and changing market dynamics have turned SOX compliance processes into a moving target, according to a Deloitte report. Mix in the reporting requirements triggered by traditional corporate activity—acquisitions, digital transformation, and entry into new markets, for instance, and it becomes clear why SOX compliance has become a complex endeavor.[2] In addition to the costs of compliance, CFOs and CEOs can face personal legal liability (up to five years in prison, or $20 million in fines[3]) for compliance failures.

But there's still time for CFOs to commemorate the law's twentieth anniversary. How? By taking the opportunity to modernize the company's end-to-end SOX program. A SOX refresh can not only help CFOs mitigate the legal peril associated with certifications but can also lower the cost of compliance. To reap the benefits, however, some finance teams must first shed an all-too-common mindset: *We've complied. What else is there to think about?*

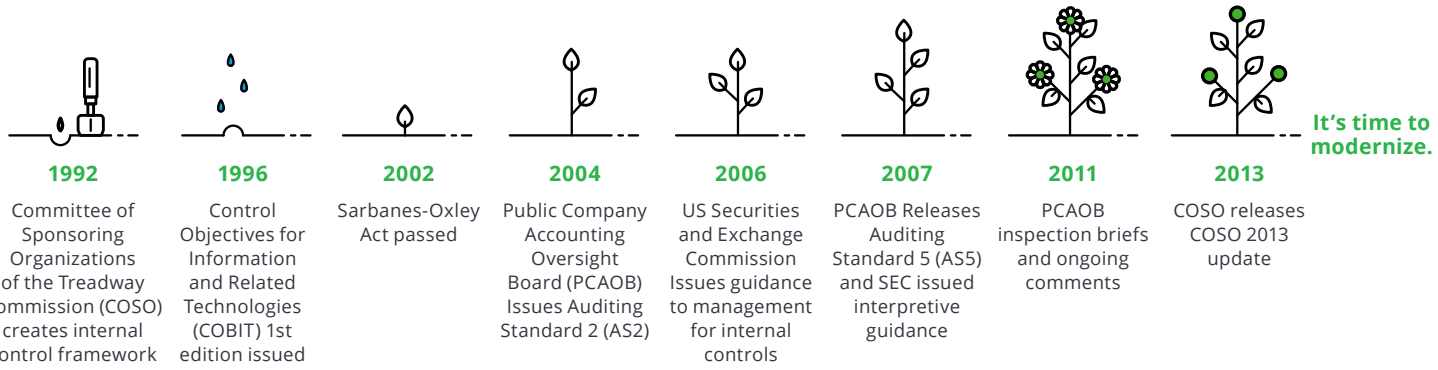
Plenty, as it turns out. In this issue of *CFO Insights*, we discuss why, 20 years after SOX became law, some companies are now saddled with outdated controls that are costly, unnecessary, and ineffective. We will also explore the steps CFOs can take to modernize their SOX programs and, by doing so, mitigate risks of material misstatement, lower the costs of compliance, improve efficiency, and gain deeper insights.

Control quality

One of the most influential and transformative pieces of federal finance regulation, SOX sought to address several exposed fault lines in the corporate governance framework, from creating greater executive accountability for financial reports, to enhancing disclosure rules, to strengthening board independence. Given its breadth, it's perhaps inevitable that compliance would grow more complex over time (see Figure 1).

Figure 1. Modern history: The Sox compliance journey

SOX was enacted in 2002, adding a layer of regulatory compliance for may SEC issuers.



It's time to refresh, rethink, and modernize the SOX program by asking these questions:

- ***How to lower the cost of compliance and still achieve regulatory obligations?***
- ***How to employ an optimized compliance framework with technology enablement?***
- ***How to harness SOX for value, not just compliance?***

Source: Sox Modernization Workshop, Deloitte & Touche LLP, 2022.

As a result, the costs associated with SOX compliance may at least in part explain why there are now more so-called "unicorn companies" (definition: private companies with valuations of at least $1 billion) than ever before.[4] (See sidebar, "SOX readiness pitfalls for companies considering IPOs.")

A top-to-bottom SOX modernization can produce savings. For example, one company reduced controls by 40% in year one and 20% in year two, which lowered costs due to testing less, among other factors. Modernization efforts should focus on the levers of transformation that follow.

Operating model optimization

Establishing an effective governance structure and maintaining clear accountability within that structure is critical. Unfortunately, some companies have left their operating structures unchanged since the years immediately following the SOX passage in 2002. Sections 302 and 906 of SOX require CFOs and CEOs to publicly certify the reliability of the financial statements being free of material misstatement. Consider including these five organizational issues:

1. What resources are needed—human and otherwise—for proper SOX compliance?
2. Do the employees responsible for controls have the requisite expertise and skills to perform their assigned tasks?
3. Is there a plan to "skill up" control owners as risk, technology, and the industry evolve?
4. If control owners do not have the requisite expertise, and training is not an option, would co-sourcing or outsourcing be beneficial in certain areas? [5]
5. Is ownership and accountability for SOX compliance driving down to the right levels of the organization?

Addressing these questions may go beyond evaluating existing controls. CFOs may need to factor in new risks such as cyber-attacks that may not have been accounted for when the company set up its SOX-related policies and practices 10 or 20 years ago. Determining if the appropriately skilled people are in place will be easier for the risks and controls that fall within the finance function. Some controls fall outside of finance and accounting, yet still have a material impact on the accuracy of the financial reports that CFOs are required to certify.

Program enhancements

Modernizing a SOX program properly means adopting a risk-based mindset that is less focused on adherence than on risks of material misstatement. For starters, take a step back and determine whether the risks that were considered relevant even as recently as the last annual risk assessment remain pertinent, or whether new risks have emerged that are not being mitigated by current controls.

The risk assessment should include both quantitative and qualitative considerations, including but not limited to:

- The degree of complexity or judgment in the process.
- The volume of activity, complexity, and homogeneity of the individual transactions.
- The frequency at which specific errors were identified in prior reporting periods.
- Whether the employees overseeing the control activities fully understand the role.
- Whether existing footnotes and disclosures in financial statements still reflect the most relevant risks.[6]

Over time, risks evolve, new risks are identified, and the organization's response may have been to design new controls without considering whether existing controls should be modified or scrapped. Companies that have grown by acquisition may have layered controls upon controls, not challenging the underlying risk assessments and failing to investigate whether some controls are now duplicative or obsolete. To mitigate risk, it's key to make sure that as threats have evolved, the needed controls have indeed been added—to address the possibility of misstatement.

Eliminating existing controls may sound perilous for CFOs responsible for attesting to the accuracy of management's report on internal controls. However, companies are not expected to maintain obsolete controls or devote the same level of resources to controls whose associated risks have declined over time. It's also possible some existing controls may have never been required in the first place, as actual regulatory requirements sometimes differ from companies' preconceived beliefs.[7] Something else to keep in mind: Under Securities and Exchange Commission (SEC) guidelines, CFOs are responsible for maintaining a control system that provides "reasonable assurance" regarding the reliability of financial reporting. Reasonable assurance acknowledges the remote possibility of misstatements and is not as high a standard as absolute assurance.[8]

Technology and automation

Some companies may still be operating their SOX compliance programs in a highly manual control environment (for signs that SOX compliance is going stale, see Figure 2).

As businesses grow and risks evolve, relying on manual controls can pose problems. It can increase program costs by siphoning employees' hours away from core operations. Also, as operating environments become more complex, manual controls may become more susceptible to human error and more vulnerable to human misconduct. Not all controls can be automated, of course, but automating some of them can help reduce such risks.

For example, many CFOs oversee high volumes of cash disbursements to suppliers and vendors. Duplicate payments can be a problem, and digital controls can help catch them. Moreover, the same technology will identify transactions that, analyzed collectively, reveal a pattern of rule breaking. For example, digital controls can flag disbursements designed to bypass authorization limits. Imagine a situation where an employee—someone only authorized to make payments of up $1 million—makes two $1 million payments to the same vendor on consecutive days.

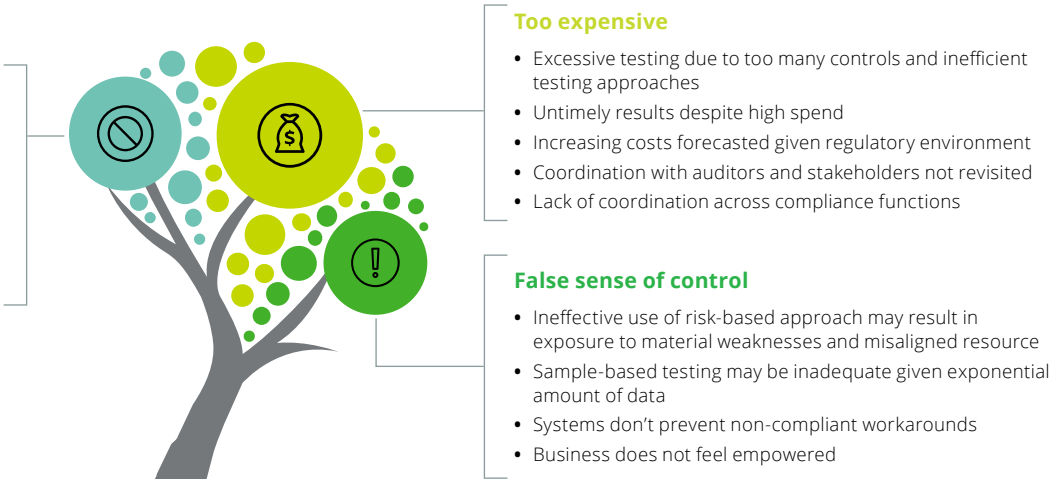
Governance, risk, and control (GRC) tools can also help improve SOX monitoring and compliance. Adoption of GRC tools has been slow, as some companies resist the cost of new software or don't see a need to abandon using spreadsheets to gather and analyze information manually. GRC tools take much of the manual monitoring out of SOX programs, creating a more reliable, streamlined information flow for CFOs. They can perform the following tasks, among others:

- Increasing accountability for risks and controls through the clear assignment of roles and responsibilities.
- Serving as a single source of truth for control documentation.
- Centralizing requests and responses related to SOX Section 302 certification.

Figure 2. Signs of a SOX program that needs a lift

Due to a lack of challenge or refresh, SOX programs have limitations and challenges. The absence of innovation for nearly two decades has resulted in some assurance functions now struggling to keep pace in a quickly changing environment.

Indicators of a stale SOX program



Source: Sox Modernization Workshop, Deloitte & Touche LLP, 2022.

- Managing documentation requests.
- Managing workflow around issues and deficiencies that have been identified.
- Providing the real-time status, through dashboard reporting, of testing and issue remediation progress.[9]

In addition to helping CFOs improve controls, reduce compliance costs, and lessen their risks of false certifications, a modernized SOX program can provide insights and value to the business beyond finance and accounting. Digital controls can add value outside the compliance function by identifying ways to operate more efficiently. By tracking payment terms and dates, analytics can help companies optimize cash flow by eliminating early payments and timing disbursements closer to when they are due.

Kickstarting a SOX refresh

Here are three steps CFOs can take now to kickstart a SOX refresh:

- **Challenge preconceived beliefs about risks and regulatory requirements**. A top-to-bottom risk reassessment may uncover regulations that no longer apply, risks that are no longer relevant, and controls that can be eliminated. Questioning old assumptions can lead to refreshed ideas and allow for companies to develop new and better ways of working.
- **Identify opportunities to automate and digitize**. If a company's SOX program or control environment has not kept up with the pace of change, then, very likely, the technology supporting the SOX program also has room for optimization.
- **Consider investment in GRC tools**. Such tools give CFOs real-team access to compliance data and to the identity of the person assigned to each control.

The cost savings and efficiency gains associated with SOX modernization can be significant. Don't wait for SOX's silver anniversary, five years from now, to take advantage.

SOX readiness pitfalls for companies considering IPOs

The number of so-called "unicorns"—private companies with valuations of $1 billion or more—has grown from 39 in 2013 to nearly 1,400 today.[10] Private companies do not have to comply with SOX, of course.

But the SEC is now considering rule changes that would require large private companies to regularly share information about their finances and operations.[11] Said SEC Commissioner Allison Lee, who has been pushing for the change, "When they're big firms, they can have a huge impact on thousands of people's lives with absolutely no visibility for investors, employees and their unions, regulators, or the public."[12]

New regulations for private companies would probably cull the unicorn herd, nudging more of them to make the leap into the public markets. But first they'd have to get ready for SOX.

Below are some SOX readiness pitfalls—many all too common and largely avoidable—that companies should watch out for:[13]

- **Trying to accomplish too much too soon**. Not determining which SOX modernization lever and activity will provide the most value to an organization and trying to do too much too fast. Being realistic about scope, budget, and timing can help you accomplish project goals more effectively.
- **Ineffective risk assessment**. If a risk assessment is not performed or not performed correctly, companies may wind up devoting too much time and too many resources to lesser risks instead of prioritizing the important ones.
- **Lack of effective communication among team members**. Set up regular communications in all aspects of your project. Provide multiple channels for interaction and have a plan for escalating issues that require attention and resolution.
- **Untimely and unplanned schedule changes**. Too many schedule changes can cause your company to miss deadlines and lose resources. Set up a formal process for managing and responding to resourcing request. Maintain a dedicated team to mitigate the risk of schedule changes.
- **Excluding people outside finance and accounting from SOX planning**. SOX has stakeholders beyond the finance and accounting functions. Make sure they have the proper training to manage internal controls.
- **Not having the appropriate skills and experiences**. Identify your go-to people for supporting the project, including external resources. Share leading practices and bring in specialized help as needed.
- **Inconsistent ways of working**. To avoid confusion and wasted time, use leading methodologies, tools, and templates so the entire SOX team can carry out their work in a consistent manner.
- **Sticking with the familiar**. Implementing a SOX program can provide a fresh opportunity to revisit laborious manual processes and replace them with automated ones that mitigate the same risks but are also efficient, sustainable, and aligned with your growth plans.

End notes

1 "Corporate Scandal Never Goes Out of Style," *Barron's*, June 30, 2022.

2 "Sox Compliance: A smarter way forward," Deloitte Development LLC, 2019.

3 SOX Section 906: Corporate Responsibility for Financial Reports, Sarbanes-Oxley-101.com, August 30, 2022.

4 "Sarbanes Oxley Turns 20," *The National Law Review*, July 19, 2022.

5 "SOX Modernization: Optimizing compliance while extracting value," Deloitte Development LLC, 2022.

6 Ibid.

7 Ibid.

8 Ibid.

9 Ibid.

10 "The Crunchbase Unicorn Board," Crunchbase News, August 12, 2022; "Going Dark: The Growth of Private Markets and the Impact on Investors and the Economy," US Securities and Exchange Commission, October 12, 2021.

11 "SEC Pushes for More Transparency from Private Companies," *The Wall Street Journal*, January 10, 2022.

12 Ibid.

13 "SOX compliance: Are you ready? A practical approach to SOX readiness," Deloitte & Touche LLP, Deloitte Development LLC, 2021.

Contacts

Theresa Koursaris
Senior Manager
Audit & Assurance
Deloitte & Touche LLP
tkoursaris@deloitte.com

Patty Salkin
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
psalkin@deloitte.com

Lindsay Rosenfeld
Managing Director
Audit & Assurance
Deloitte & Touche LLP
linrosenfeld@deloitte.com

Sandra Teixeira
Managing Director
Risk and Financial Advisory
Deloitte & Touche LLP
sateixeira@deloitte.com

About Deloitte's CFO Program
The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject-matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career—helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

For more information about Deloitte's CFO program visit our website at:
www.deloitte.com/us/thecfoprogram.
Follow us @deloittecfo

Deloitte *CFO Insights* are developed with the guidance of Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; Josh Hyatt, Manager/CE Journalist, CFO Program, Deloitte LLP; and Jon Birger, Manager/CE Journalist, CFO Program, Deloitte LLP.