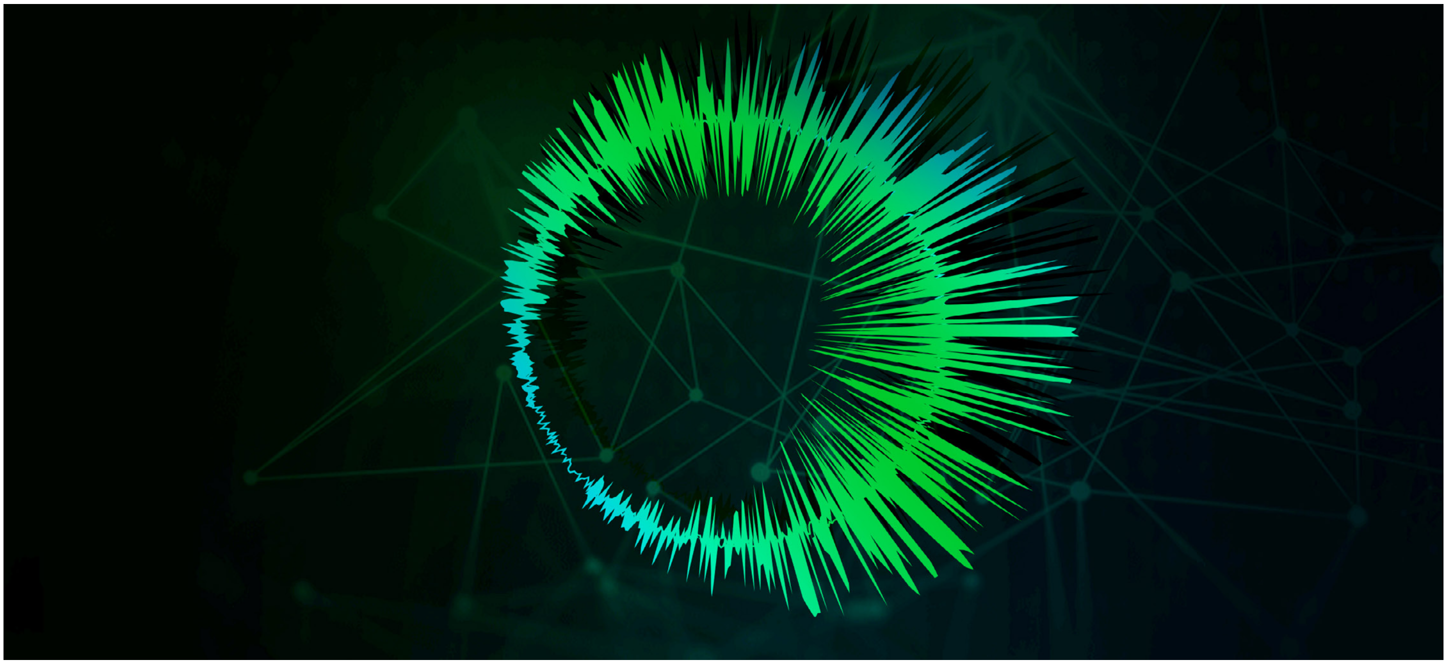
Deloitte.



SOX modernization: Optimizing compliance while extracting value

It’s time to refresh and rethink SOX

Many programs and processes at companies can succumb to the proverbial saying, “if it ain’t broke, don’t fix it.” This can be exacerbated by competing priorities due to an evolving business environment, new or revised regulatory requirements, changing technology, and so on. For many public companies, the program established to comply with the regulatory requirements of the Sarbanes-Oxley Act of 2002 (SOX) may have also fallen into a “rinse and repeat” pattern.

In the years since this federal law was enacted, there have been significant developments in technology, methodology, and business and operating environments; however, the SOX program at many companies may not have evolved at the same pace, or at all. Over the years, some SOX programs may have even continued to layer on additional controls while spending the same amount or more to achieve compliance without being able to extract value from the program.

A SOX program that has not been challenged in years may be stale, which could be a drain on resources and impede performance, particularly if this compliance program is treated more like a “check-the-box” activity. Organizations in this scenario could be testing too many controls or may not be focused on the areas that matter most, so they may not actually be attaining reasonable assurance over the operating effectiveness of internal control over financial reporting (ICFR). This could ultimately result in unexpected deficiencies or even material weaknesses.

After having an established SOX program for years, especially one that may not have kept up with the pace of change, it’s time to refresh, rethink, and modernize the SOX program. Through modernization, a company can optimize its SOX program, achieve efficiencies, extract value and insights to share with other areas of the organization, and potentially lower the related cost of compliance while still achieving reasonable assurance for regulatory compliance.

SOX modernization goes beyond controls rationalization to also consider operating model optimization, program enhancements, and technology and automation opportunities. Depending on an organization’s specific facts and circumstances and where it is on its SOX journey, different aspects of each of these pillars may be implemented at different times to effectively drive modernization.

Operating model optimization

An established governance structure and clear accountability are fundamental to an effective operating model. Unfortunately, these areas may not always be well defined and should be periodically revisited, especially given the variety of stakeholders throughout the organization required to support SOX compliance beyond the finance and accounting functions. It is important to remember that although SOX is related to ICFR, inputs into the financial reports are also from the business, so responsibility over the operation of internal controls extends to those relevant business processes, systems, and applications.

Defining the overall governance structure of the SOX compliance program can help to ensure there is oversight by those resources with the appropriate skill set and level of authority to drive the strategic vision of the SOX program and effectively and efficiently communicate those decisions to all relevant stakeholders.

As each stakeholder performs their respective role, a monitoring program should be in place to be able to track where controls are not operating effectively, or risks are not being appropriately mitigated. The monitoring program should be risk-based and align with the risk assessment, so time spent investigating any issues or deficiencies identified is prioritized to the areas where the organization should be spending the most focus.

The SOX program should seek to drive accountability. For control owners, this accountability should be related not just to their respective controls, but also the identified risks that those controls were designed to mitigate. If the focus is just on controls, existing controls may not consistently mitigate the related risk, especially as risks within the organization change, and could also lead to the testing of controls that are not relevant to address related risks. If the focus shifts to the risk, stakeholders have an opportunity to drive change to focus on those controls that mitigate that risk more effectively and efficiently.

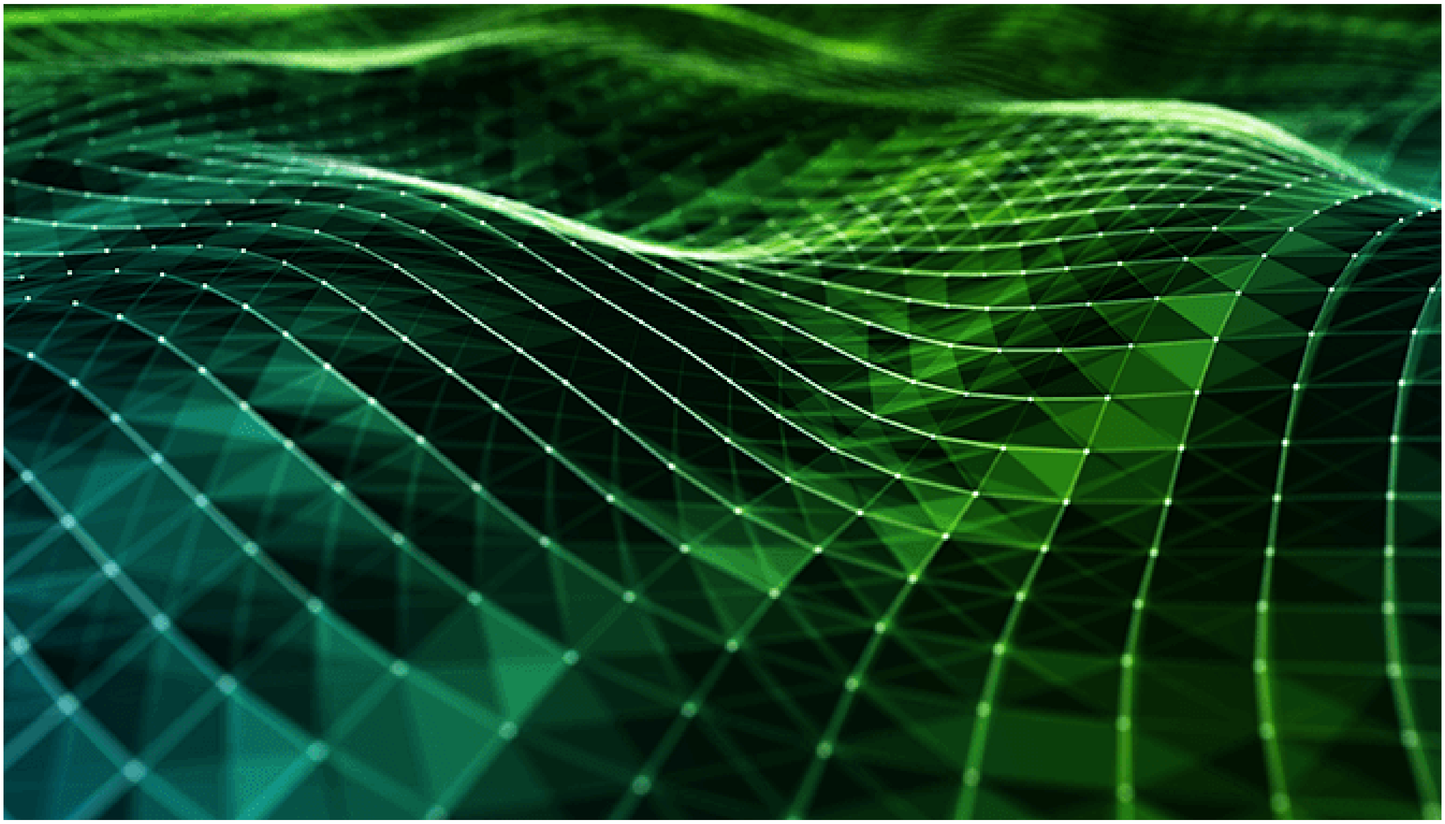
> A SOX program that has not been challenged in years may be stale, which could be a drain on resources and impede performance, particularly if this compliance program is treated more like a “check-the-box” activity.

Another approach to optimizing the operating structure is to consider how and when resources should be involved in the SOX program and to remain flexible in that regard. When determining who should be involved in the SOX program and defining their related roles and responsibilities, the company should consider leveraging the Institute of Internal Auditors (IIA) Three Lines Model, which clarifies the roles and duties that different groups throughout the organization could have in managing risk for the company.

Some questions to contemplate when reconsidering the SOX program structure at an organization include:

- What resources are needed, and how can those resources be flexible across compliance?
- Do current resources have the required expertise?
- Should there be a dedicated pool of resources in-house, and should they be centralized or global teams?
- Would a co-sourcing or outsourcing model be beneficial in certain areas?
- How can SOX resources and control owners continue to be up-skilled as risk, technology, and the industry evolves?

Determining what combination of resources could be most effective for a company would be based on its specific facts and circumstances and would require judgment. A company may also transition between these resource options at various points in time depending on its current situation.



Program enhancements

When identifying opportunities to modernize a SOX program, it's important to take a step back and challenge what is being performed, especially in relation to what is required. Part of this process would also include a refreshed understanding of the requirements and related guidance.

One of the requirements of SOX Section 404(a) includes that management is responsible for establishing and maintaining an adequate internal control structure and evaluating that internal control structure based on certain criteria.

In addition, the Securities and Exchange Commission (SEC) published interpretive guidance for management regarding its evaluation and assessment of its internal control structure. In this interpretive guidance, the SEC indicates that

"Management is responsible for maintaining a system of internal control over financial reporting ("ICFR") that provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles." [1]

Management's responsibilities related to internal control over financial reporting is to obtain reasonable assurance over the reliability of financial reporting, not absolute assurance, and the concept of "reasonableness" is objective with a range of judgments and methodologies that could be considered appropriate. Performing an effective risk assessment can help management identify areas with risks of material misstatement within the company and determine which of those areas it should focus its efforts.

Many factors could contribute to a lagging SOX program. Over time, risks evolve, or new risks are identified, and the response may have been to design new controls without always taking into consideration if any existing controls should be modified or removed. Additionally, once risks are identified, the level of risk may not be considered, such as if it's a lower risk or a significant risk, which could result in not spending enough time in areas of significant risk or spending too much time in areas of lower risk. Controls could also have been added to manage an issue or deficiency identified without actually addressing the root cause.

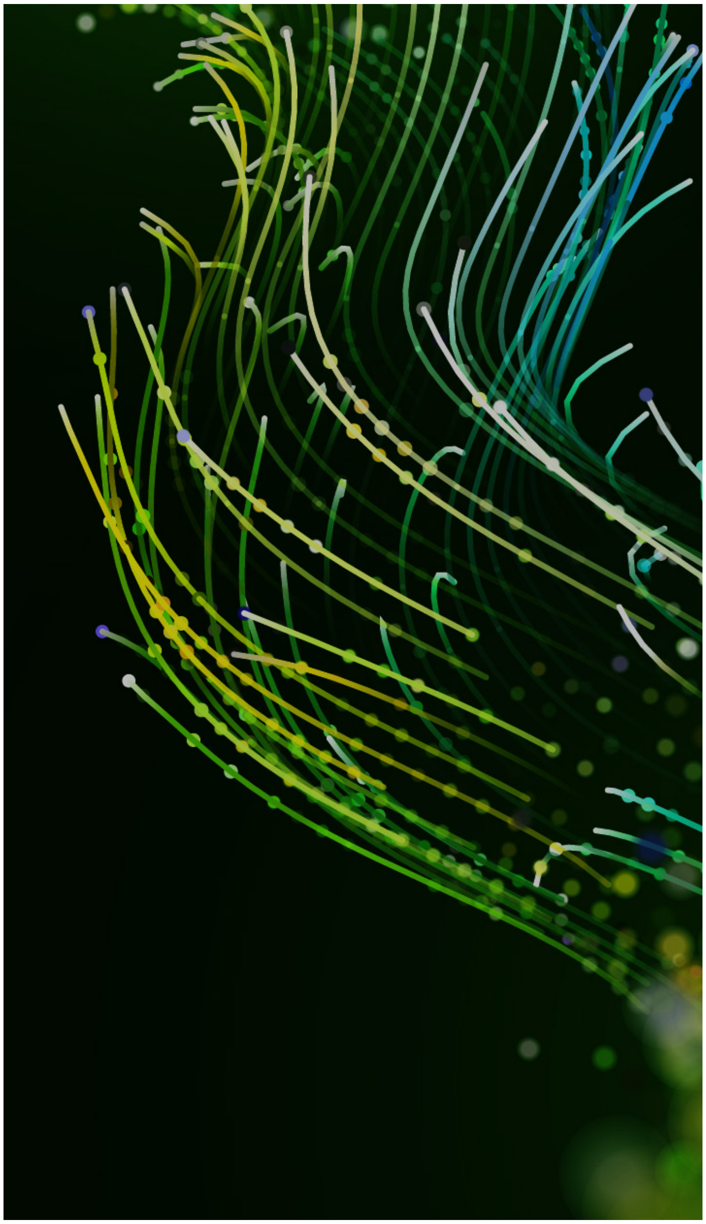
This could also impact how companies remediate issues and control deficiencies. Not all control deficiencies should be considered equal as some control deficiencies may need to be remediated more urgently than others. If the company tries to remediate all control deficiencies without considering the risk level, they may not remediate those with the highest impact in a timely manner.

Endnote

[1] SEC Interpretive Release: Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934.

After years of complying with SOX, some companies may no longer perform a robust risk assessment through a critical lens and may end up focusing more on identifying the controls that will be subject to testing in the current year, performing the testing of design and operating effectiveness of those controls, and evaluating results. For example, the control environment at a company may change, such as a significant nonrecurring transaction, and may not adequately identify new risks and mitigating controls associated with that transaction.

There are other activities that should happen to lead up to selecting the controls to be subject to testing—the actual risk assessment. Refreshing the risk assessment from the beginning and evaluating each step of the risk assessment through a critical lens can help to determine if there is a shift in which areas that company should focus on due to new or changed risks.



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

- Degree of complexity or judgment in the process
- Volume of activity, complexity, and homogeneity of the individual transactions
- Prior period errors identified
- Whether the resources performing the control activities are new to the role
- Footnotes and disclosures
- Assessment at a more granular level, such as the business unit level

To be able to prioritize areas of focus, as risks are identified the risk level should be considered to distinguish those risks that, if left unmitigated, could lead to a material misstatement in the financial statements.

Once risks are identified and prioritized, controls designed to mitigate those risks to achieve reasonable assurance can also be identified. At this point, there is an opportunity to think critically about the controls identified for testing based on the areas of focus prioritized in the risk assessment to determine if new controls are needed to address a new or changed risk and if existing controls need to be modified or are no longer needed.

As the risk assessment is being performed, the company should also consider the potential for fraud as well as the dependency on information technology and outsourced service providers and the related risks and controls.

As a company continues down the path of SOX modernization, there is an opportunity for companies to harmonize their risk assessment efforts beyond just internal control over financial reporting across other compliance activities throughout the organization. These other areas may also be performing their own risk assessments to meet different objectives for financial reporting, operations, or compliance, and there could be risks in these other areas that overlap or even feed into the risk assessment for SOX. Companies have an opportunity to perform an assessment to determine where collaboration among functions would benefit the organization and further drive integration of compliance activities across the organization, including breaking down silos, having those cross-functional conversations, and leveraging data to be able to identify trends and create visualizations to gain deeper insights and add value.

Technology and automation opportunities

Many companies may also face the challenge of a highly manual control environment. 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. These challenges may result in increased program cost, both due to the increase in controls and the increase in deficiencies identified due to the manual nature of company processes.

Identifying opportunities to automate and digitize can support a company's efforts to modernize its SOX program. Leveraging technology can enable a SOX program in a variety of ways and can lead to enhanced quality, increased efficiency, deeper insights, and can potentially reduce the total cost of compliance.

One option for automation is to automate the testing of controls. Many companies have not automated their controls monitoring and rely on point-in-time, sample-based testing resulting in manual reviews. This execution method of testing is also typically applied as a wholesale approach and may not always take into consideration areas of focus and risk level to differentiate the level of effort. Automated testing consists of profiling certain populations and transactions with real-time results, allowing a company to be able to test up to 100 percent of the population and potentially achieve more assurance for less time and cost. Even with automated controls testing, the company would still need to perform exception and trend monitoring to be able to respond to any exceptions in control performance.

Another option for automation is to automate controls. Automated controls are inherently more reliable than manual controls when they are designed appropriately, and there is less opportunity for human error once implemented. There are two ways to think about control automation:

1. Automate the manual control itself.
2. Implement new automated controls, such as higher-level direct and precise monitoring controls, for example, that profile populations of data that are high volume and low dollar amount to identify risks and outliers in the population.

These types of digital controls modernize the design, implementation, and controls testing capabilities and proactively trigger corrective actions that mitigate exposure and reduce residual risk.

Not all controls can or should be automated, so a company would have to decide which controls should be automated. When determining which controls to automate, the following steps should be followed:

1. **Plan** – Identify the stakeholders, project scope, milestones, and deliverables for the project to automate controls.
2. **Rationalize** – Validate the plan around which control activities to select to automate and what risks to focus on.
3. **Automate** – Implement the control automation techniques.

A third option for automation is to automate an entire process, which is considered revolutionary. Just like controls, not all processes can or should be automated, so a company would have to decide which processes would be beneficial to automate. A primary consideration in making the determination of which process has the most potential to be automated is to consider whether it is a highly manual process that occurs frequently and is defined by a standard set of activities. Automating processes could contribute to liberating resources to handle more complex tasks, reducing errors by removing human interaction, and reduce time and cost by having a more efficient process. This would also allow a company to rationalize the controls over that process since the automation implemented should help reduce the associated risk related to that process.

An additional route enabling the benefits of technology is to implement a governance, risk, and control (GRC) tool. A GRC tool can empower an organization to manage and streamline its SOX program and compliance risk overall. For example, it can:

- **Serve as the single source of truth** for control documentation.
- **Manage documentation requests** and related control testing.
- **Manage workflow** around issues and deficiencies identified.
- **Centralize requests and responses** related to SOX Section 302 to support certification.
- **Provide real-time status** of testing and issue remediation progress.
- **Enhance visibility and reporting** by leveraging visualization dashboards.
- **Increase accountability** through assignments of roles and responsibilities.

Where to go from here

As companies consider opportunities for modernization, they should revisit what the actual regulatory requirements are versus any preconceived beliefs of what is required. Sometimes these beliefs don't align with the actual requirements, and over time, they can begin to be accepted as facts and become roadblocks for moving forward. Challenging some of these beliefs can lead to refreshed ideas and allow for companies to develop new and better ways of working.

With organizations continuously looking to do more with less, simply having a compliance program that doesn't provide additional business insights should not be considered a sustainable option. By refreshing and modernizing the SOX program, a company can identify opportunities to increase efficiency, shift focus and efforts to areas that matter most, potentially reduce the cost of compliance, and extract value and provide insights to other areas of the organization beyond finance and accounting, all while still achieving compliance.

To learn more about how SOX modernization can help your organization, contact us.

Authors:

Lindsay Rosenfeld
Partner, Audit & Assurance
Deloitte & Touche LLP
linrosenfeld@deloitte.com
+1 313 396 3167

Theresa Koursaris
Senior Manager, Audit & Assurance
Deloitte & Touche LLP
tkoursaris@deloitte.com
+1 212 492 3666

Patricia Salkin
Managing Director, Risk and Financial Advisory
Deloitte & Touche LLP
psalkin@deloitte.com
+1 732 890 6003

Sandra Teixeira
Managing Director, Risk and Financial Advisory
Deloitte & Touche LLP
sateixeira@deloitte.com
+1 212 436 2523

Deloitte.

The services described herein are illustrative in nature and are intended to demonstrate our experience and capabilities in these areas; however, due to independence restrictions that may apply to audit clients (including affiliates) of Deloitte & Touche LLP, we may be unable to provide certain services based on individual facts and circumstances. This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services.

This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services, which provides advisory services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2022 Deloitte Development LLC. All rights reserved.