

## SOX compliance: Are you ready?

### A practical approach to SOX readiness

When companies make the decision to enter the public market, whether through a traditional initial public offering (IPO) or through a special-purpose acquisition company (SPAC), they all have one thing in common—they must all comply with the Sarbanes-Oxley Act of 2002 (SOX). With all the competing priorities and other requirements of a public offering, focusing on becoming SOX compliant may be challenging to balance. While compliance with this federal regulation has been a requirement for publicly traded companies for years, companies may still struggle with how to practically prepare for and comply with SOX.




In this article, we'll explore what compliance with SOX can practically mean for a company and how a company can become SOX ready by focusing on people, process, and technology.

#### First, the background

SOX is a United States federal law enacted on July 30, 2002, that mandated several reforms to enhance corporate responsibility and financial disclosures, as well as to combat corporate and accounting fraud. Among other things, SOX established the Public Company Accounting Oversight Board (PCAOB), strengthened penalties for corporate fraud, established certain internal control requirements for management, and established certain requirements for independent auditors to attest to management's assessment of internal controls.

For a better understanding of what's required for a company to be SOX compliant and generally when it's required, let's focus on Sections 302, 404, and 906 (figure 1).

Figure 1. Sarbanes-Oxley Sections 302, 404, and 906 requirements

When a company decides to become public, it will have to meet the Sarbanes-Oxley requirements for management certifications:		
<div><div>Section 302 Certification overview</div></div> <p>CEO and CFO to make specific certifications as of the end of each <b>quarterly</b> and <b>annual</b> reporting period, including:</p> <ul style="list-style-type: none"><li>• Report contains no untrue statements</li><li>• Report is fairly presented in all material respects</li><li>• Responsibility for design and maintenance of disclosure controls and procedures as well as internal controls over financial reporting</li><li>• Not based on a specific criteria (approach based on risk)</li></ul> <div>Required from first quarterly filing</div>	<div><div>Section 404 Overview</div></div> <p>CEO and CFO are required to document and assess as of the end of every <b>annual</b> reporting period:</p> <ul style="list-style-type: none"><li>• Their responsibility for establishing, maintaining, and testing effective internal control over financial reporting</li><li>• Their assessment of internal controls 404(a), accompanied by the independent auditors' attestation report 404(b)</li><li>• Their assessment is based on specific criteria (i.e., COSO)</li></ul> <div>Required from second annual report</div>	<div><div>Section 906 Certification overview</div></div> <ul style="list-style-type: none"><li>• CEO and CFO to make certifications that all financial reports—including <b>annual</b> and <b>periodic</b> reports—fairly present, in all material respects, the financial condition and results of operations of the issuer and that they conform and comply with the Act</li><li>• Provides for significant criminal penalties for noncompliance</li></ul> <div>Required from first quarterly filing</div>

The timing of when these sections are applicable to your company can depend on your company's specific facts and circumstances. The maturity of your current internal control environment, the number of disparate financial reporting systems, the number of locations, and myriad other nuances can all affect how long it takes to become SOX compliant. It is recommended to consult with legal counsel when in doubt.



Figure 2. An illustrative timeline to achieve SOX compliance goals is shown in the below graphic.

Illustrative timeline to achieve SOX compliance goals:	12 months prior	6 months prior	IPO date	1st 10-Q	Subsequent 10-Qs	1st 10-K	2nd 10-K
<b>Management responsibilities</b>							
Sections 302 <sup>1</sup> and 906—CEO and CFO certification				●	●	●	●
Section 404(a)—Management's report on the effectiveness of ICFR <sup>2</sup>							●
Section 404(b)—Independent auditors' attestation on the company's effectiveness of ICFR <sup>2,3</sup>							●

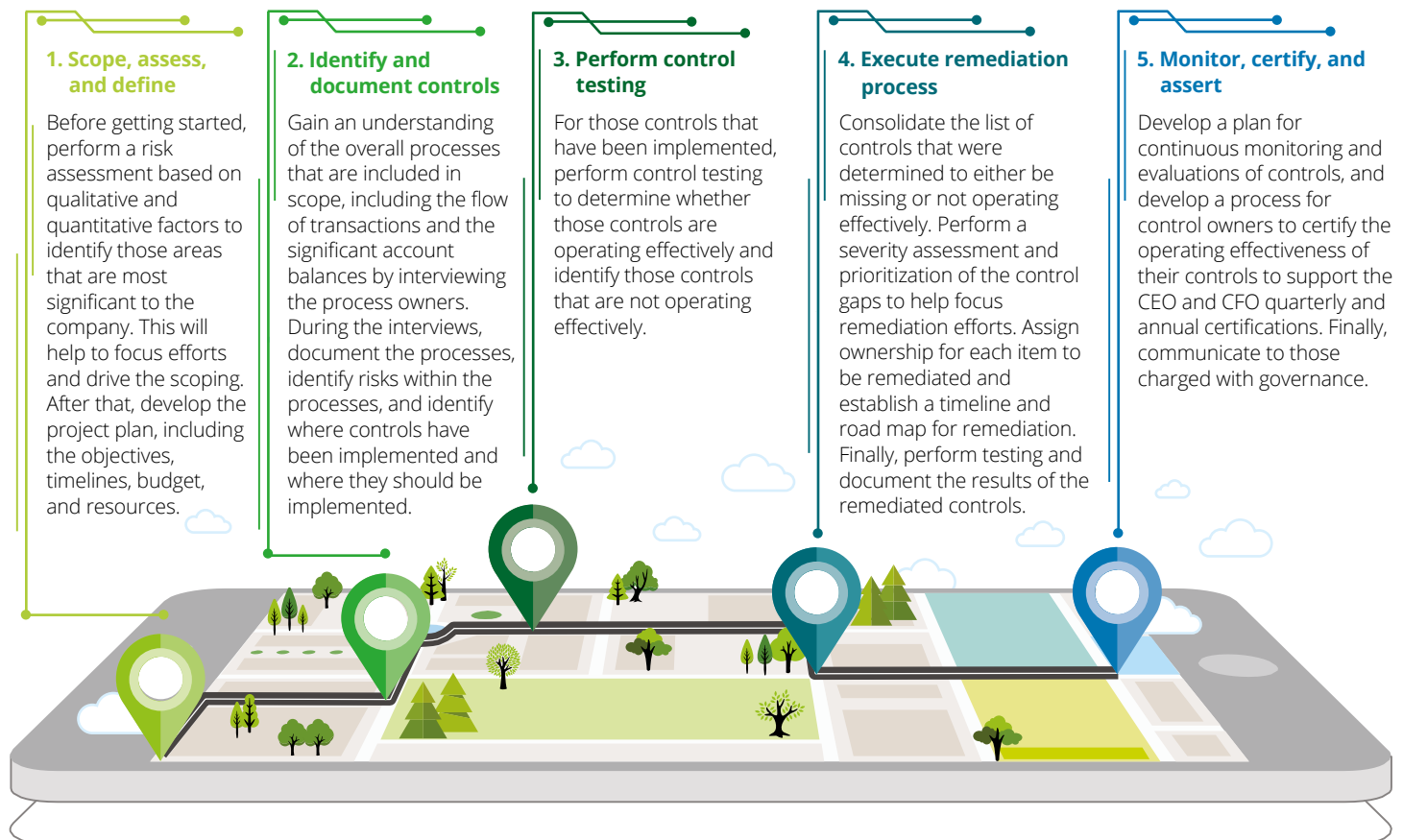
1. Until the company is required to comply with SOX Section 404, the chief executive officer (CEO) and chief financial officer (CFO) may omit the portion of the introductory language in paragraph 4, as well as language in paragraph 4(b), of the certification that refers to their responsibility for designing, establishing, and maintaining internal control over financial reporting.<sup>1</sup>
2. For companies that become public through a SPAC transaction, the timing of management's report on the effectiveness of internal control over financial reporting (ICFR) may be different. In the scenario where the SPAC, which is already a public entity, has filed its first Form 10-K and then subsequently acquires a target company, that target company usually takes over operations of the public entity. At the end of the reporting period following the acquisition, the company will essentially have to file its second Form 10-K, where management's report on the effectiveness of ICFR is required. Therefore, these companies may have a shorter runway for when they need to comply with SOX Section 404, unless they are able to take the SEC SOX exemption. Consultation with accounting advisers and legal counsel is strongly recommended.
3. The timing of the independent auditors' attestation on the company's effectiveness of ICFR typically aligns with management's report on ICFR and is also required for the newly public company's second Form 10-K. However, the requirement for the independent auditors' attestation on the company's effectiveness of ICFR may be further out depending on the company's filing status. For example, the independent auditors' attestation on the company's effectiveness of ICFR is not required for companies that meet emerging growth company (EGC) filing status.

1. Title 17: Commodity and Securities Exchanges, Part 240—General Rules and Regulations, Securities Exchange Act of 1934, [https://www.ecfr.gov/cgi-bin/text-idx?SID=30da76ab97612d5b10ba77694a2c0628&mc=true&node=se17.4.240\\_113a\\_614&rgn=div8](https://www.ecfr.gov/cgi-bin/text-idx?SID=30da76ab97612d5b10ba77694a2c0628&mc=true&node=se17.4.240_113a_614&rgn=div8).

## The road to SOX compliance

The road to SOX compliance may seem long and daunting, especially considering the expanse of who needs to be involved, what is included, and the repercussions if it's not done appropriately. One way to tackle this is to break it down into phases to better manage the overall process (figure 3).

Figure 3. Five phases of SOX compliance



As a company continues down the path of SOX compliance, it's important to consider progression through these phases. Phase 1 **Scope, assess, and define** will help companies identify their areas of greatest risk. When they do this, they are able to narrow down their focus and better define where they should be spending their time.

Once a company has determined where they should focus their efforts, they are better equipped to move to phase 2 **Identify and document controls**. At this point, companies are able to get started by obtaining an understanding of those areas identified in phase 1 to identify controls that are relevant to address risks of material misstatement. To the extent that companies determine that controls are missing (i.e., gaps) or are not properly designed to fully mitigate risk, they can jump directly to phase 4 **Execute remediation process** and prioritize where to remediate gaps or unmitigated risks. Since

the requirements for SOX Sections 302 and 906 are not based on a prescriptive framework, the results of the analysis performed during these phases can provide relevant information for the CEO and CFO as they sign their quarterly and annual certifications.

As companies move into phase 3 **Perform control testing**, they will then be able to perform testing around the operating effectiveness of controls that were appropriately designed. If any controls are deemed to not be operating effectively, management can move forward to phase 4 **Execute remediation process**, but this time the focus shifts to prioritizing and remediating the deficiencies related to how controls are operating. Remember, since not all control gaps are considered equal, some control gaps may need to be remediated more urgently than others. Performing a severity assessment and prioritization of the control gaps will help to focus remediation efforts.

Finally, phase 5 can typically be performed throughout the process as management develops and executes a plan for continuous monitoring and a process for control owners to periodically certify the operating effectiveness of their controls. The results of the analysis performed during these phases can provide relevant information for management’s annual report on the effectiveness of ICFR.

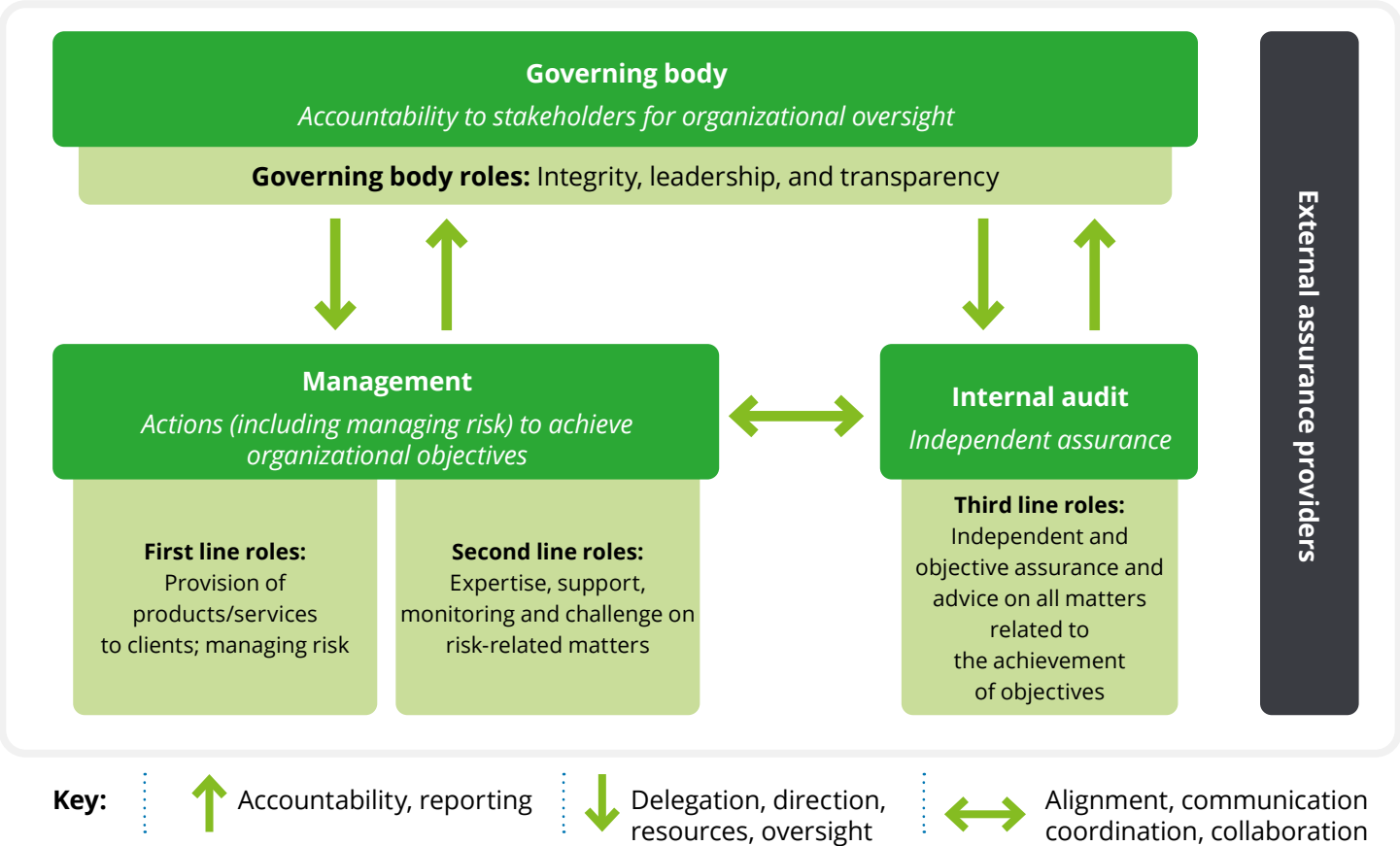
Focus on people

When developing and maintaining an internal control framework, it’s critical to have resources with the appropriate skill set and level of authority within the accounting and finance areas, but also throughout the organization. Even though SOX is focused on ICFR, it’s important to keep in mind that inputs into the financial reports are also from the business, so controls are also needed over relevant business processes, systems, and applications. This means that the responsibility for effective internal controls reaches beyond just finance and accounting and into other areas of an organization, and training is an important component of communicating roles and responsibilities over SOX throughout the organization.

When considering who should be involved in the SOX program, 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 have in managing risk for the company.

Determining how to operationalize this model to meet the needs of an individual organization takes judgment. Specifically related to the second and third lines in figure 4, companies early in their SOX compliance journey may not have in-house resources available with the requisite skills to perform the duties of these roles. Additionally, the second line could exist in an organization in a variety of ways, such as a stand-alone SOX compliance department, as part of a Risk and Compliance group, or another group as determined by the company. Companies that don’t have any resources available for these functions may want to consider starting with an outsourcing model to quickly obtain the resources necessary to fill the gaps to work toward compliance. An outsourcing model is when a service provider with the necessary experience is contracted to perform the required tasks.

Figure 4. Institute of Internal Auditors (IIA) Three Lines Model



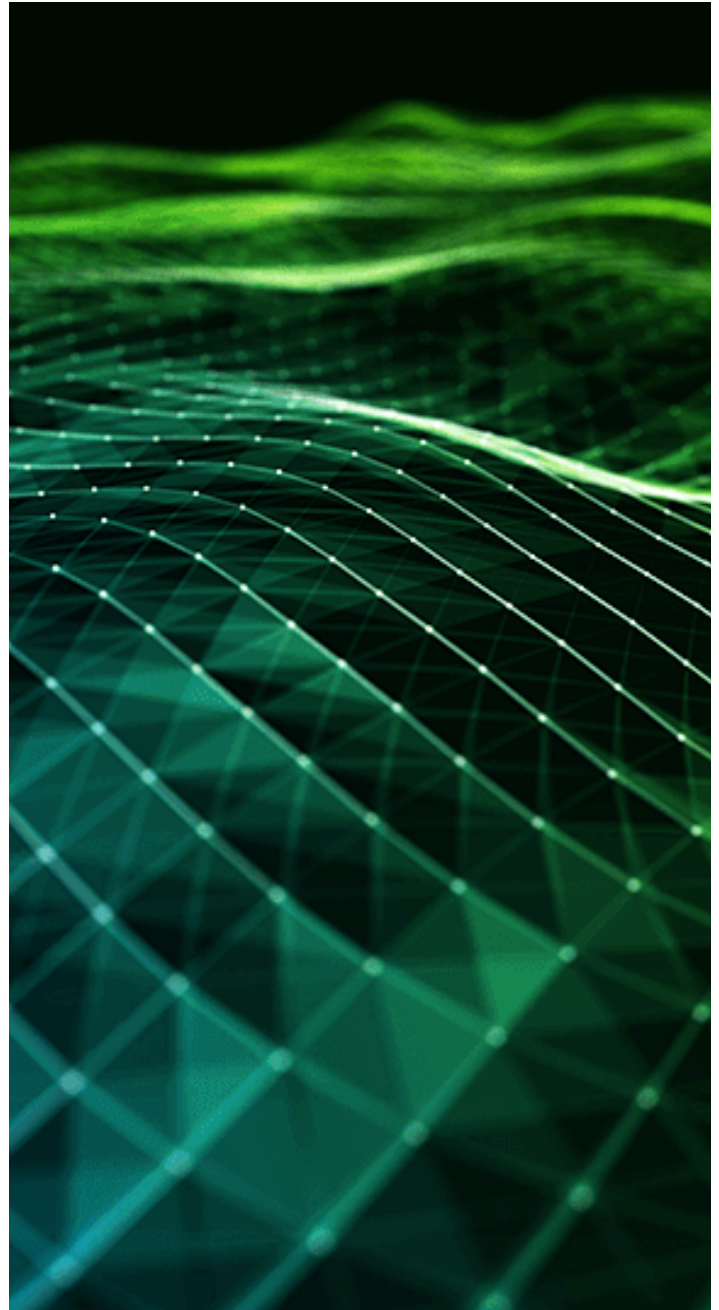


Alternatively, if there are some in-house resources available, a company may want to consider a co-sourcing model. In a co-sourcing model, a service provider is also contracted to perform certain tasks but works alongside in-house resources already there.

Either of these models could be beneficial to get personnel with the required experience quickly and to also provide training and support for the existing in-house resources. If a company opts to start with an outsourced model, for example, they could, over time, move toward a co-sourced model and eventually to a full in-house model, if that is their preference. Again, the purpose of this model is to clearly define the roles and responsibilities related to an effective SOX program throughout an organization and as a company's SOX program matures, they may transition between these operating models at different points in time.

The CEO and CFO of an organization should be particularly interested in ensuring that resources with the appropriate skill set and level of authority are involved in the SOX program. As mentioned earlier, the CEO and CFO sign SOX Section 302 and 906 certifications within the company's quarterly and annual filings with the SEC, but what does this really mean? In these certifications, the CEO and CFO are both signing a personal statement in accordance with the requirements listed in SOX Sections 302 and 906 listed in figure 1. If the certification submitted is not accurate or the CEO or CFO does not comply with the requirements, regardless of whether it was done mistakenly or deliberately, the CEO and/or CFO is personally subject to criminal and financial penalties.

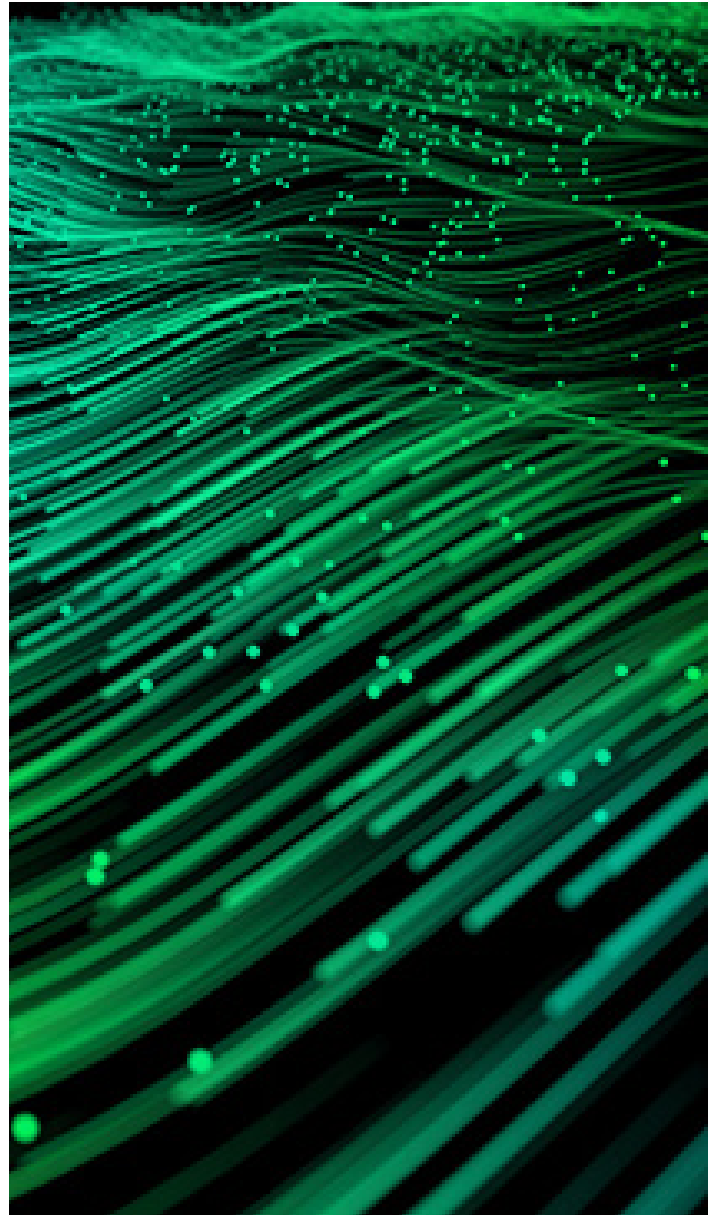
What should the CEO and CFO do to gather relevant information in preparation to sign these quarterly certifications? A common practice in public companies is to leverage the first and second lines by implementing a quarterly control certification process at the control owner level. This not only drives ownership of controls into lower levels of management throughout the organization but also provides for a timely opportunity for control owners and management to identify and escalate any concerns related to their internal controls or notify leadership of significant changes to the control environment. Since these control certifications would come from multiple control owners throughout the organization, a dedicated function (for instance, the SOX compliance team) typically would coordinate the distribution of the certifications, as well as the accumulation and evaluation of the responses, in order to provide the requisite information to the CEO and CFO, so they are able to more confidently sign their quarterly certifications.



### Focus on process

As mentioned earlier, 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, or a framework. The most commonly used framework is the 2013 Internal Control – Integrated Framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).<sup>2</sup> COSO established the five components of an effective internal control framework, which are defined as follows:

- 1 Control Environment** – “The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.”
- 2 Risk Assessment** – “Involves a dynamic and iterative process for identifying and analyzing risks to the achievement of objectives.”
- 3 Control Activities** – “The actions established through policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out.”
- 4 Information and Communication** – “Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives.”  
“Communication is the continual, iterative process of providing, sharing, and obtaining necessary information.”
- 5 Monitoring Activities** – “Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control is present and functioning.”



2. <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf>.

Most process-level controls are typically found within the Control Activities component. Although ensuring that internal controls are appropriately designed and implemented for significant processes is important, equally as important is spending time developing those entity level controls that would address the other four components.

To support the achievement of SOX compliance, it's important to embrace changes that may need to occur throughout the organization. As previously noted, a key factor to consider is that SOX compliance goes beyond just the finance and accounting departments. It starts with the tone at the top; that is, the commitment by the CEO, CFO, and leadership of a company to establish and drive an open, honest, and ethically sound corporate culture. The tone and behavior demonstrated by leadership impacts the behavior and standard of expectations throughout the company. Establishing a tone at the top enforcing the importance of internal control is an important entity-level control for a company. Additional entity-level controls that should have the attention of leadership include establishing clear reporting lines; attracting, developing, training, and retaining competent individuals; and developing a process to gather and distribute information as appropriate, among others.

Another important entity-level control that should have management's attention sooner rather than later is performing a risk assessment. Performing a risk assessment can help to identify those areas with risks of material misstatement within the company. This can help further define those areas where management may want to focus their efforts, based on a specified materiality. An effective risk assessment should be iterative, include both quantitative and qualitative considerations, go beyond the financial statements to also consider the related footnotes and disclosures, and consider business controls as well as general information technology controls over relevant systems and applications. Additionally, performing a risk assessment is not a one-time event, especially since the CEO and CFO will need to sign quarterly and annual certifications attesting to the operating effectiveness of controls.

Finally, don't forget the importance of a monitoring program. After spending time and effort implementing controls to become SOX compliant, monitoring helps to ensure you remain compliant and can help identify any deficiencies or areas for improvement.

### Focus on technology

When standing up a system of internal control for the first time, there will likely be control gaps identified. It's possible to remediate these gaps by designing manual controls. However, before you do that, consider your technology options.

Technology not only can help you comply with SOX by implementing controls to mitigate risks but also can generate organizational efficiencies and improve operations. Automated controls are inherently more reliable than manual controls when they are designed appropriately, and there is less opportunity for human error once implemented.

Additionally, many companies already have technology solutions in place but may not be leveraging them to their fullest extent. For instance, companies often discover unused capabilities in their enterprise resource planning (ERP) systems that they can enhance to further support their control environment.

In addition to considering automation at the process level, companies should explore opportunities for automation related to the management of their SOX framework by leveraging a governance, risk, and compliance (GRC) technology platform. GRC tools can help a company implement their SOX framework, manage workflow around control testing and deficiency remediation, and support the ongoing monitoring of their framework overall. This type of automation helps to instill accountability and ownership throughout the organization because the GRC solution centralizes the documentation of the controls and tags the associated control owner. GRC tools also typically include dashboards with real-time updates of control-testing progress and any related gaps identified, allowing for a more efficient and effective issue resolution process.

Whether at the process level or managing the internal control framework through the use of a GRC solution, automation can offer the CEO and CFO greater confidence that the certifications they're signing reflect more accurate, real-time information.



### Common SOX readiness pitfalls to avoid

Like any project, SOX implementation has its challenges. Although some may be unexpected or unique to the company's situation, many others are all too common—and largely avoidable. Here are several to watch out for.

- **Trying to accomplish too much, too soon** – Moving too fast can put a heavy burden on company resources. Being realistic about the scope, budget, and timing can help you accomplish your project goals more effectively.
- **Ineffective risk assessment and scoping** – If a risk assessment is not performed or is not effective, there is the potential for a company to spend a disproportionate amount of time and effort in areas of less risk instead of prioritizing areas of greater risk.
- **Lack of effective communication among team members** – Set up regular communication in all aspects of your project. Provide multiple channels for interaction, and have a way to escalate issues that require attention and resolution.
- **Failing to coordinate with external auditors** – Meet with external auditors up front so they know about your project, including the conclusions of your risk assessment, the controls you chose, and how you designed them.
- **Untimely and unplanned schedule changes** – Too many schedule changes can cause you to miss deadlines and lose resources. Set up a formal process for managing and responding quickly to resourcing requests, and maintain a dedicated core team to mitigate the risk of schedule changes.
- **Excluding people outside finance and accounting** – SOX has stakeholders beyond the financial and accounting functions. Keep them in the communication loop and provide sufficient training over SOX requirements and how that will change their day-to-day way of executing and evidencing their internal controls.
- **Not having the appropriate skills and experiences** – Identify your go-to people for supporting the project, including external resources that can work across your business, 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 SOX team can carry out their work in a consistent manner.
- **Sticking with the familiar** – Implementing SOX can provide a fresh opportunity to revisit existing laborious manual processes and controls that protect against the current known risks and replace them with automation that can mitigate the same risks, but are also efficient and sustainable in alignment with your growth plans.

### A practical path forward

The Sarbanes-Oxley Act of 2002 (SOX) represents the most comprehensive reform of capital markets legislation since the 1930s' Securities Acts. When it became law in 2002, its aim was to restore investor confidence in financial statements of public companies by creating new rules for corporate governance, disclosure, and reporting.

The law's most prominent provisions for internal control are Sections 302, 404, and 906, which require the CEO and CFO to make specific certifications related to the company's financial reporting and for management to report on the operating effectiveness of relevant controls at a point in time. Becoming compliant with these and other provisions is a significant undertaking that includes assigning new roles and responsibilities for risk management, the selection and application of an internal control framework, and consideration of technology solutions for a more accurate, timely picture of the control environment. Breaking the endeavor down into phases can make it more manageable, as can taking an iterative, agile approach that tackles the highest priorities first and allows for continuous learning and improvement.

Although this article covers a lot of ground, every company has its own set of facts and circumstances that add nuance to a company becoming SOX compliant. For further discussion, please feel free to contact any of the authors.

## 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

### Contributors:

**Michelle Donahue**

Managing Director, Audit & Assurance Deloitte  
& Touche LLP  
midonahue@deloitte.com  
+1 203 563 2556

**Rohit Chhajer**

Senior Vice President, Audit & Assurance  
Deloitte & Touche LLP  
rchhajer@deloitte.com

**Patrick Stultz**

Senior Manager, Audit & Assurance  
Deloitte & Touche LLP  
pstultz@deloitte.com  
+1 704 227 7925

### Special thanks:

**Stuart Rubin**

Managing Director, Risk and Financial Advisory  
Deloitte & Touche LLP  
stuartrubin@deloitte.com  
+1 561 962 7826

**Patricia Salkin**

Managing Director, Risk and Financial Advisory  
Deloitte & Touche LLP  
psalkin@deloitte.com  
+1 609 806 7279



[Accounting Advisory & Transformation Services](#)



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](http://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 © 2021 Deloitte Development LLC. All rights reserved.