The IT SOX and IPO journey

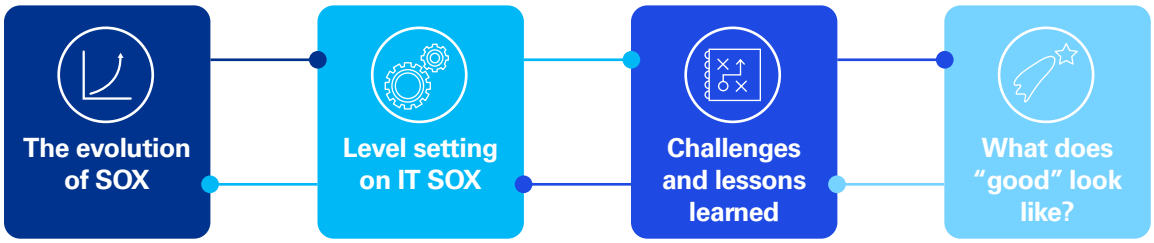
Application Risk webcast
Original airdate: August 3, 2022

Webcast summary

Effective SOX programs offer benefits that go beyond compliance. Establishing a robust system of internal IT controls can help companies prepare for SOX as well as serve as a springboard for IPO success by developing a sound system of governance and risk management that enables responsible growth.

The webcast discussed the evolution of SOX and highlighted the critical factors for building a successful IT SOX compliance program to get IPO-ready.

The panelists addressed the following topics:



The evolution of SOX

Implemented in response to significant corporate accounting failures and frauds, the Sarbanes-Oxley Act of 2002 (SOX) aims to restore shareholder value and bolster trust in capital markets. SOX is arranged into 11 sections covering wide-ranging topics, from auditor independence, corporate responsibility, and enhanced financial disclosures to corporate fraud accountability and the creation of the Public Company Accounting Oversight Board. There are, however, four SOX sections that are crucial for newly public companies:

- SOX 302 and SOX 906 are both executive certifications. Section 302 mandates that senior officers of a public company, most often the chief executive officer and chief financial officer, certify that all reports are accurate, complete, and fairly represented and affirm that all the necessary disclosures are made.

  Section 906 addresses criminal penalties for certifying a misleading financial report. These are the first applicable sections after initial public offering (IPO) effectiveness—required with the first periodic report filed with the Securities and Exchange Commission (SEC) post-IPO.

- Under Section 404, management and external auditors are required to report on the adequacy of financial reporting controls. Section 404(a) demonstrates management's annual assessment of the design and effectiveness of their internal controls over financial reporting. It is disclosed in the company's annual report stating the management's responsibility, the framework used, and their conclusion. If the controls are found to be ineffective due to the presence of a material weakness or more than one material weakness, then there are additional disclosures needed around remediation of those deficiencies.

Additionally, 404(b) is an external auditor's attestation of the company's internal controls over financial reporting, stating whether your controls were effective or ineffective. Both 404(a) and 404(b) are not required for newly public companies until the second annual report post-IPO effectiveness.

- Milestones in achieving a SOX-ready state:
  - The year-one journey of IPO effectiveness starts with the S-1 filing date, which is a registration statement filed with the SEC verifying that the financial statements and all the disclosures—including material weaknesses—have been reviewed and eventually declared effective.
  - Post-IPO effectiveness date, there is a two-year succession of 10-Ks or annual reports. Due to the transition period allowed by the SEC, the first 10-K would only require a very brief disclosure stating that management's assessment of controls is not included.
  - From the second year, Section 404 kicks in. If you're an Emerging Growth Company based on the criteria outlined in The Jobs Act, you are required to continue to comply with 404(a) only. Companies considered "Large Accelerated Filers" need to comply with both 404(a) and 404(b). The auditor would conduct an integrated audit of the internal controls and provide an opinion on them in the second-year post-IPO, unlike the first year when controls are assumed to be under development.

How SPAC differs from traditional IPO

Special-purpose acquisition companies (SPACs) face an accelerated schedule to address competing priorities as opposed to traditional pre-IPO companies, which typically take a year or more to get IPO-ready. In SPAC mergers, companies need to meet the same regulatory requirements as pre-IPO companies, but in a much shorter timeframe. In such scenarios, multiple variables determine the SEC requirements based on the timing of the merger in that fiscal year, adding complication. Therefore, it's better to focus on the traditional IPO timeline.

Level setting on how IT affects SOX

The overarching purpose of SOX is to correct any material or structural weakness in corporate governance and oversight policies to increase public confidence that key financial reports are accurate. Information technology (IT) teams are increasingly crucial in obtaining this assurance, as they are heavily responsible for configuring an appropriate controls framework that supports internal controls over financial reporting.

What are the bare minimum IT controls needed?

There is no "one size fits all." To comply with SOX, companies need to go through a risk assessment and scoping process, all driven through their financial statements. There's a materiality exercise to determine what is material to your organization based on which you can link your business processes to those disclosures and start identifying the areas that are reliant on IT.

It's crucial to understand that SOX requires you to have IT controls over financial reporting risks rather than everything in the IT environment. These IT controls are focused on enabling businesses to manage operational risks; comply with regulations; and ascertain confidentiality, integrity, and accuracy of information. These objectives are bolstered by:

- IT Application Controls (ITACs) operate within a business process that manages your financial statement reporting risk and relies on technology. These controls are usually fully automated and verify accurate initiation, recording, processing, and reporting of financial data in specific systems. Examples include segregation of duties, interfaces, input controls, validation checks, and approval workflows.
- IT General Controls (ITGCs) operate around the systems that are in scope for SOX. These are baseline IT controls that govern the security, management, development, and maintenance of operating technology systems.

  Without foundational ITGCs, it is difficult to rely on the effectiveness of critical ITACs that are directly linked to financial statement assertions. Examples include access to programs and data, approach to provisioning and deprovisioning, implementing changes to control processes, managing and monitoring integrations, and controls over system implementations and upgrades.
- Information Produced by the Entity (IPE) Controls include information such as key business process reports, audit logs that are leveraged to execute controls and provide audit evidence. From an IT standpoint, it's crucial to have controls that validate the completeness and accuracy of IPE, whether for use in the execution of internal controls or supporting controls testing.

Besides these, there are governance and oversight controls, which include entity-level controls, policies, and procedures that support a company's business models and establish risk tolerance.

Challenges and lessons learned

There are many complexities that organizations typically face during an IPO journey. In the course of their IPO, founders and executives need to build robust internal systems and controls environment. From our experiences working with private companies embarking on their IPO, we've identified a few common challenges and pitfalls that interfere with their SOX compliance.

Top challenges in the controls landscape

- Reliance on disparate systems, managed by multiple stakeholders, makes it difficult to manage information efficiently and often results in decentralized governance and issues with the integrity of financial reporting data.
- Legacy systems may not be able to support effective SOX-compliant reporting processes, which is raising the stakes on application modernization.
- Migrating to cloud-based infrastructure—applications that are configuration-centric—is not enough. It's important to invest in capabilities to understand how to set up and support such applications, otherwise this may lead to inadequate design and execution of key IT SOX controls.
- Organizations that are going public have a significant amount of cloud utilization for which they rely on third-party vendors. It's important to understand the shared responsibility model and establish appropriate third-party oversight controls to demonstrate appropriate governance over the financial reporting risks that the third party is managing for you.

Common constraints and pitfalls:

- Most private organizations don't have the resources, both in terms of capacity and controls capability, to assess, remediate, design, and execute a compliant SOX program–and many start too late to establish the program in time for their first year of 404.
- Bandwidth-constrained IT teams deprioritize controls due to competing project work, and hence fail to adequately support the IT SOX journey.
- Undefined ownership or lack of clarity with regard to who owns which control itself lends to fragmented collaboration. SOX finance/IT teams need to work together and understand their shared responsibilities.
- Weak access controls and separation of duties (SoD) means there may be pervasive IT issues that have to be addressed before an effective control framework can be designed.

What does "good" look like?

- The journey to SOX readiness is focused on:
  - Planning your controls around the SOX-IT landscape
  - Assessing your current state to identify gaps
  - Remediating the gaps in the control environment
  - Operating the controls as part of business as usual
  - Testing the controls for validation. This is where Sections 404(a) and 404(b) come into play.
- Additionally, you might move to more automation in your control environment to make it more efficient and less reliant on manual processes, which are more prone to error.
- Five critical success factors include:
  - Scoping the program appropriately such that it is risk-aligned and focused on what matters for financial reporting
  - Having adequate PMO resources, internally and externally, to drive ownership and collaboration
  - Having sufficient internal sponsorship, funding, and accountability for change management
  - Equipping teams with technology and application expertise to manage security and controls efficiently
  - Aligning your SOX program with your external auditor.
- During transformation, a "good" controls program consists of the following phases:
  - **Phase1**–Assessment and Baseline: Design what your "future-state" should look like. Review and identify opportunities for improvements to ITAC, ITGC, and IPE controls.
  - **Phase2**–Remediate – Controls Analysis and Design: Design action plans to expand on Phase 1 results to close gaps and standardize policies, procedures, and controls.
  - **Phase3**–Controls Testing: Validate design and effectiveness. Document and verify policy, procedure, and control changes.
  - **Phase4**–Ongoing support: Test controls landscape periodically to confirm ongoing compliance. Review processes and metrics regularly to benchmark against key performance indicators and optimize where possible.

Closing comments

Companies that decide to go public must comply with SOX. However, it can be challenging to balance the competing priorities of a public offering with preparing for SOX compliance. IT SOX readiness can help break silos, automate controls to mitigate risks, and meet reporting standards while positioning companies for IPO success.

Contacts

Neal Bradsher
Partner,
Internal Audit & Enterprise Risk
KPMG LLP
P: 612-305-5700
E: nbradsher@kpmg.com

Richard Knight
Principal and U.S. IT–Internal Audit Solutions Leader,
KPMG LLP
P: 703-286-8393
E: raknight@kpmg.com

Christian Leva
Managing Director,
GRC Technology Services
KPMG LLP
P: 214-840-2000
E: cleva@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia