Future of SOX Webcast: The State of SOX

September 22, 2022

Webcast summary

As companies focus on maintaining a strong internal control over financial reporting (ICOFR) environment, accelerating the adoption of technology in the execution of controls and in the control testing is key to drive efficiency and effectiveness and to deliver a robust, cost-effective program.

The webcast highlights the results and themes identified in the KPMG 2022 SOX survey and discusses the best practices for implementing and utilizing governance, risk and compliance (GRC) tools to create efficiencies and insights into SOX programs.

The panelists discussed the following topics:

- KPMG 2022 SOX survey highlights
- Best practices for Implementing and utilizing GRC tools
- Trends in material weaknesses for IPO and non-IPO companies

KPMG 2022 SOX survey highlights

Almost two decades of ICOFR compliance experience has positioned experience has positioned SOX functions to become controls advisors to the organization—providing practical, real-time input on how to modify controls to address and leverage rapidly changing technology environment to drive efficiency and effectiveness. The KPMG SOX survey 2022 compiled industry data to identify the current internal controls over financial reporting (ICOFR) trends, challenges, and strategies:

SOX Program structure and strategy: Organizations have shifted the strategic focus of their SOX program over the past five years from minimizing SOX compliance costs and solely focusing on maximizing external auditor control reliance, to optimizing their control portfolios and improving their business processes.

- Higher reliance on technology as compared to 2016: utilizing data analytics to identify anomalies from a risk perspective; embedding automation and testing bots in the SOX program to reduce manual tasks and to promote more insights.
- Increased focus on continuous monitoring—particularly in the IT general control areas.

Technologies utilized in the SOX program: Organizations are increasingly adopting technologies to reduce levels of administrative tasks such as status updates, and also allowing more real time insights into control status.

There has been a massive increase in the use of GRC tools from 2016 (41 percent) to 2022 (69 percent)

External auditor reliance: With increased demands for cost effectiveness of the execution of testing of the ICFR environment, there has been an increase in focus on achieving reliance of external auditors on SOX controls testing performed by internal audit or management testing teams. This was crucial to ensure efficiency from cost as well as control owners time perspective.

- 85 percent of organizations indicated that their external auditor place reliance on their work compared to only 41 percent in 2016
- Around 63 percent of respondents reported that external auditors relied on 21–60 percent of their operating effectiveness testing.

SOX key and non-key controls:

- Although the percentage of in-scope automated controls remained consistent from 2016 to 2022, the percentage of in-scope IT Dependent controls increased 28 percent and the percentage of manual controls decreased 31 percent over the same time frame
- Large-size (revenue over $50 billion) companies account for the highest percentage of total automated controls.

Average spends per controls: Organizations of all sizes are focused on monitoring the costs of internal controls over financial reporting (ICOFR).

- Across all organization sizes in 2022, transaction controls with more than 20 samples have the highest average testing hours at 16 hours per control.
- The significant drivers of increased testing time include IT General Control (ITGC) and management review control (MRC).

SOX risk assessment factors:

- The covid-19 pandemic was a major driver of cloud migrations and digital acceleration. As a result, system implementations and process reengineering efforts is cited as the top SOX risk assessment factor for 2022 rather than transactional factors (fraud in day-to-day activities and financial statement line level) in 2016.
- Other risk assessment factors include acquisitions, divestitures, and reorganizations, regulatory changes, new business initiatives, and new or superseded accounting pronouncements.

SOX program improvement focus areas:

- By organization revenue size: Improving the quality of control evidence and communications with external auditors are the two top focus areas for small-size companies, followed by increasing external auditor reliance. Whereas large-size companies are more focused on communication with management, followed by reducing in-scope control counts and enhancing risk and control descriptions
- By industry: The highest number of activities across all industries is around improving the quality of control evidence, particularly in the banking and capital markets. While financial services and the technology and software markets are most concerned with controls optimization. The common themes identified across industries include increase in control automation, driving external auditor reliance, and reducing the in-scope control count.
- Organizations with control owners who understand the risks in their control and can articulate the control activities and how those activities mitigate the risk along with good documentation to support it, can enhance the entire SOX process, which, in turn, helps drive efficiency and reduce costs.

Audit committee communication:

- The major focus is on communication concerning control exceptions and sustainable remediation efforts, which are primarily communicated at a higher level.

Best practices for implementing and utilizing GRC tools

Achieving sustainable growth and improving business conduct, through transforming the risk function, is key to operating in today's environment. Organizations need to look at risk transformation journeys through different aspects of the business—such as technology, data, process, and people—to think holistically when approaching their GRC technology implementations and unlock new opportunities.

At KPMG, we see GRC platforms and frameworks as an approach to align the organization's governance, risk, and compliance processes to its strategy, allowing for convergence and transparency of information to drive performance and resilience in a dynamic economic business environment. We follow a six-pronged approach to all our GRC implementations:

Vision and strategy: A strong program to manage risk and compliance requires a vision of what a new GRC program is designed to achieve for the organization—what success looks like.

- The vision must address business needs and strategically align with the organization's overall objectives
- It is advisable to create measurable success criteria and obtain stakeholder buy-in and commitment at the onset.

Program management: Once the roadmap is instituted, it is important to establish robust program governance and change management process to align the stakeholders and clearly define roles, responsibilities, and accountabilities.

- Communicating regularly with project stakeholders is one of the best practices to confirm expectations and enable the effective planning and maintenance of tasks and resources
- Identifying and assigning tasks to stakeholders enables transparency and effective monitoring of progress, dependencies, and risks.

Vendor selection: The GRC technology landscape is broad and complex. There could be various technologies worth evaluating for your organization, depending on your current and future needs.

- It is a common mistake for companies to focus solely on one technology. A fair evaluation of technology vendors is essential to ensure their cultural fit with the organization
- Participating in a detailed demo of the technology and investing time upfront to document high-level business requirements helps align with future needs of the organization with the program.

Convergence and data architecture: One of the common pitfalls is that organizations do not think critically about their data architecture and how it drives downstream reporting.

- Data is a very important part of any implementation; hence, it is critical to review and validate data architecture such that reporting functions are successfully enabled
- Analytics and continuous control and monitoring are key to setting up the architecture appropriately and identifying opportunities for improvement and alignment with the target state data architecture.

People and change: The key to any implementation program hinges upon the users effectively using the system. It is important to prioritize developing a user training strategy to address changes and empower end users to operate the systems efficiently.

- Organizations need to have a communication strategy in place that conveys the success criteria and communicates the rationale for change consistently to all key stakeholders.

Technology enablement: With data analytics and artificial intelligence redefining GRC practices, the adoption of emerging technology is the key to transforming a SOX function. Technology-enabled solutions are helping integrate, streamline, and maximize the efficiency of an organization's GRC strategy and enabling informed decision-making to assist SOX program management and execution.

- First and foremost, it is important to understand that business requirements should be designed with the end in mind. Companies must review current state reports, rationalize, and develop requirements for technology enablement and align stakeholders on the desired outcome of GRC technology
- Developing detailed user acceptance testing procedures and documenting defects can help align and validate business requirements.

An effective implementation often entails significant changes to the way people do their work. Many stakeholders may be reluctant to change; therefore, a successful GRC journey starts with a stakeholder needs assessment, followed by targeted stakeholder engagement and then, expectation management. The roadmap should enable the vision and consider the maturity of the functions to be enabled and the speed of adoption. In addition, consideration should be given to 'quick wins' to show progress and to create positive momentum. This is critical to allow visibility of the program, facilitate communications, and budget for costs. Companies setting up the SOX program for the first time should consider implementing GRC tools once they've set up a reasonably stable set of key controls and the initial risks and control matrix.

Closing comments

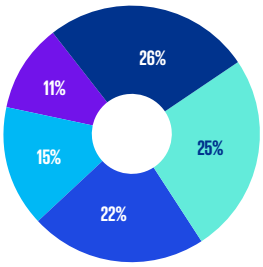
Building a new GRC program is a complex undertaking that involves many moving parts and a wide array of corporate departments. For many organizations, it has been a costly and painful endeavor to establish an integrated GRC, due to a range of causes, including lack of strategy, poor executive buy-in, failed software implementations, poor change management, and a lack of alignment between program outcome and stakeholder expectations. Organizations need to understand that it is possible to develop a successful GRC program provided they adopt certain good program practices. A robust GRC program will not only improve the way companies manage risk and compliance but also improve business operations.

Trends in material weaknesses for IPO and non-IPO companies

- Of the 3,366 annual reports filed in 2021, 193 companies (6 percent) disclosed material weaknesses in their filings. The unique number of companies filing reports with material weaknesses for 2021 continues to be slightly lower than pre-2020 levels due to the SEC's amended accelerated filer definition effective April 2020.
- Although material weaknesses are more likely to occur in small companies that are still maturing from a control perspective, about 8 percent of companies have reported issues related to restatement of company filings. The top five primary themes in 2021 that applied to 20 percent or more companies reporting material weaknesses include:
  - Lack of formal documentation, policies, and procedures
  - Lack of accounting resources and expertise—typically an issue in newly public companies
  - IT, software, security, and access issues—more prevalent in companies that have gone through a recent implementation or upgrade
  - Lack of segregation of duties/design of controls—increasingly seen in both newly public companies and accelerated filers
  - Inadequate disclosure controls

It is important to note that material weaknesses are not all equal in severity. There may be times when a company has one material weakness, which is relatively easy to remediate and remove the following year. But a broad material weakness or multiple material weaknesses may result in a multi-year journey to be able to fully remidiate. Consequently, companies should perform a thorough risk assessment and ensure controls are designed and performed by competent personnel without overlooking the technology aspect of financial reporting. A strong IT team and well-implemented and controlled systems are critical in ensuring internal controls over financial reporting.

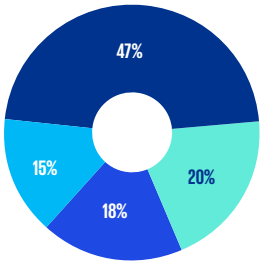
What is the size of your organization (revenue)?



- <$100m
- $100m - $2bn
- $2-10bn
- $10bn - $50bn
- $50bn+

1775 responses

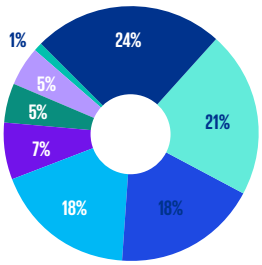
How engaged is your Audit Committee in the details related to your Sox program?



- Low: Only report major issues such as potential MW's, disagreements with auditors, risk to not completing the annual SOX program etc
- Moderate: Quarterly status report on progress of testing, key themes related to control failures and status of remediation
- High: Detailed quarterly status report
- N/A

1955 responses

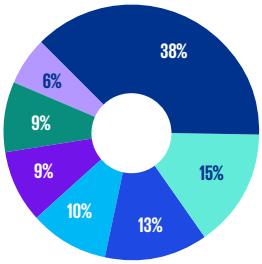
Which technology do you use in your SOX program?



- MS Excel
- AuditBoard
- Workiva
- Other
- SharePoint
- RSA Archer
- Custom in-house build
- ServiceNow

2000 responses

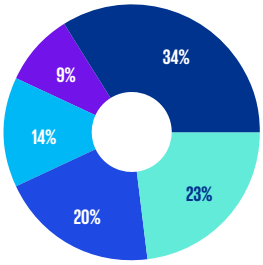
What is your biggest focus for 2022



- Improve quality of control performance and/or increase automation of the control
- Increase use of Data Analytics in SOX program
- Communication/coordination with external auditors
- Reduce number of in scope controls
- Reduce control testing/cost
- Increase reliance by external auditors
- Other

1932 responses

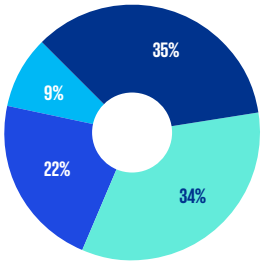
Does your GRC Technology increase the efficiency of your SOX program



- Yes, Estimate 10-20% time saved
- Yes, Estimate up to 10% time saved
- Yes, Estimate 20%+ time saved
- No time savings
- N/A

1860 responses

Have you been able to utilize the data from your GRC tool to drive risk assessment activities



- Not yet, but that's our objective
- Yes, able to assess control owner turnover, changes in control design etc. and use that to drive risk assessment and testing strategy
- No, we don't think that's feasible and/or don't want to change our approach
- N/A

1774 responses

Contacts

Sue King
Partner and SOX
Solutions Lead

Ethan Beardslee
Director,
GRC Technology

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