Unlocking value beyond compliance in your SOX program

Global SOX survey results

EY

Building a better
working world

Background

Much has happened since the introduction of Sarbanes-Oxley Act (SOX) in the early 2000s. Since the initial passage in the United States in 2002, legislation akin to SOX has been passed in several countries, including Japan, Canada, South Africa and Korea. Additionally, countries such as the United Kingdom and the Netherlands are considering similar internal control regulations.

There's no question that the pace of change and disruption in today's environment is fast, yet slow — faster than it has ever been and slower than it will ever be in the future. Rapid convergence of industries, new business models, increasing regulation and an evolving workforce are all underpinned by advances in technology. Groundbreaking discoveries such as artificial intelligence and robotics bring about increased efficiency while introducing new and heightening current risks.

As leading organizations continue to innovate and transform business for the future, their approach to internal controls also needs to be more progressive. But how much progress is being made today?

We conducted a global SOX survey to examine how organizations are managing and enhancing SOX, what challenges they are experiencing and how technology is being used globally. Survey respondents included a wide range of publicly traded companies of various sizes from around the world, of whom 80% have complied with SOX or similar legislation for more than five years.

Respondent overview by size

34%
Revenue greater than $10b

47%
Revenue between $1b and $10b

19%
Revenue less than $1b

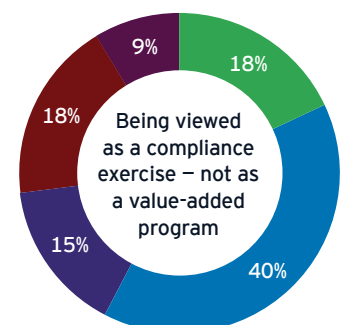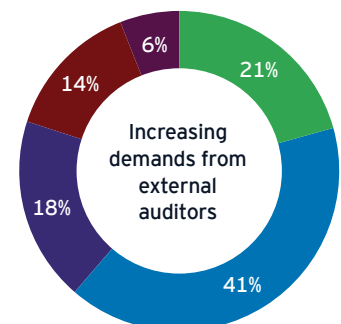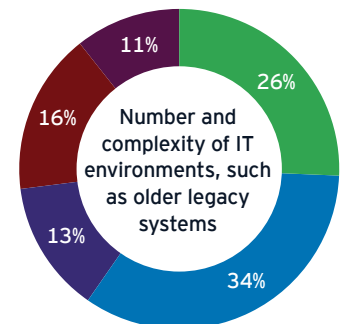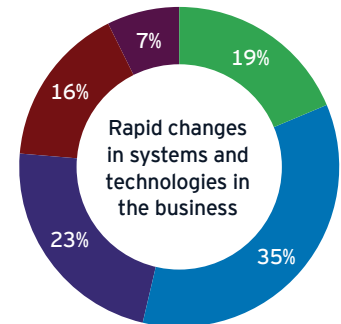## Respondents' headquarter locations
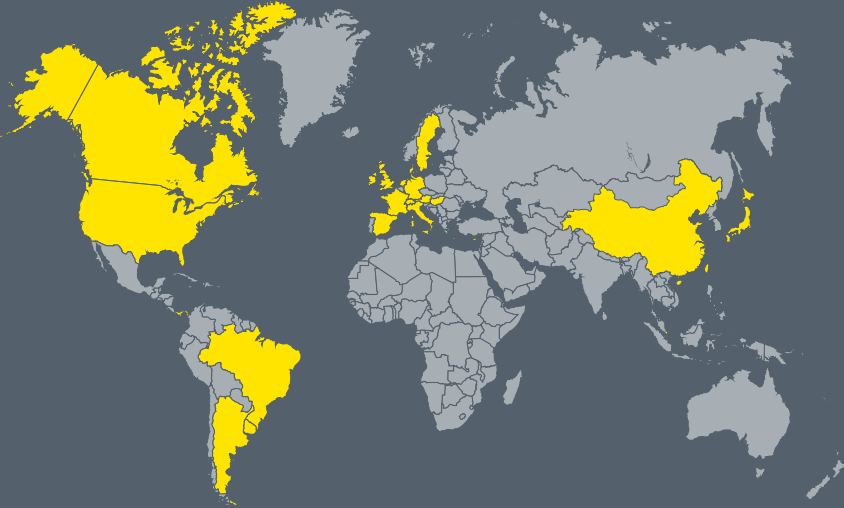
By its very nature of being a legislative requirement, SOX is viewed as a compliance effort at its core. More than 87% of the survey respondents agree, believing their main objective is to maintain a lean, effective internal controls framework focused on internal and external risks. The majority are also focused on achieving significant reliance on management's work by the external auditors.

However, SOX can add value to a company if the objectives are focused in the right places. Organizations are beginning to look for synergies between SOX efforts and overall governance, risk and compliance (GRC). This alignment and coordination of risk activities across the business helps embed SOX in the daily routine of the control owners and makes it less of a stand-alone compliance initiative.

More than 37% of companies have gone a step further to leverage SOX as a way to enhance management skills, experience and accountability over controls. Having a strong internal controls framework and trusted operating environment at the foundation creates a safety net, allowing organizations to spend less time making sure the operations are functioning as intended and more time focused on leveraging risk to drive reward and growth.

With these objectives in mind and the advances made in business and technology over the last 20 years, one would expect to see efficiencies in the overall process and program. However, 63% of respondents say that the level of effort to execute SOX has actually increased, and 16% stated it has remained the same since initial implementation. These statistics make it difficult to say that organizations are getting the full value out of their SOX programs.

> **Looking deeper into the primary challenges organizations are facing today, respondents noted the most significant challenges impacting their control environment include:**
>
> ‣ Rapid changes in systems and technologies utilized by the business
> ‣ Number and complexity of information technology (IT) environments, such as older legacy systems
> ‣ Increasing demands from external auditors
> ‣ Being viewed as a compliance exercise – not as a value-added program

Now that we better understand the challenges contributing to these metrics – how do we move past them?	The EY survey uncovered three common themes and opportunities:
	Importance of strong, connected governance and oversight
	Responsive and risk-based operating model enabled by technology
	Continuous program improvement

Q: Which of the following challenges are you currently facing within your control environment?

Rapid changes in systems and technologies in the business
7% | 19% | 35% | 23% | 16%

Number and complexity of IT environments, such as older legacy systems
11% | 26% | 34% | 13% | 16%

Increasing demands from external auditors
6% | 21% | 41% | 18% | 14%

Being viewed as a compliance exercise – not as a value-added program
9% | 18% | 40% | 15% | 18%

Key

- 🟩 Very significant
- 🟦 Significant
- 🟪 Neutral
- 🟥 Somewhat significant
- 🟪 Not significant

Importance of strong, connected governance and oversight

Tone at the top is imperative to reinforce key objectives, adherence to program requirements and effective change management, yet only 36% of SOX program structures have a formal steering committee in place that is composed of all key stakeholders. The majority of respondents are split in their approach on what subset of stakeholders, if any, oversees the coordination and decision-making processes governing internal controls in their organization. Expanding the steering committee to include other functions outside of the controllership, IT and internal audit improves stakeholder alignment and enables others to understand the activities and how they can be leveraged to drive value – not just compliance. This also makes executing SOX easier, as the business understands the compliance and business purpose behind control performance and testing.
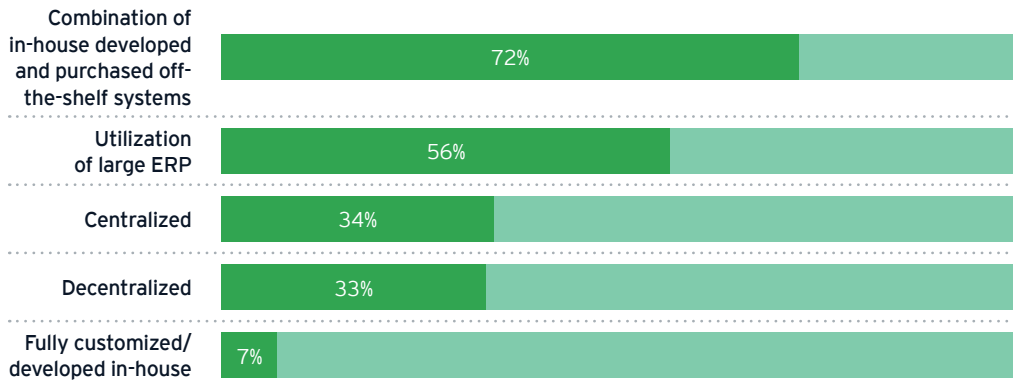
Achieving a high-quality, effective and efficient level of SOX compliance requires a more holistic approach to program management, especially for organizations that are navigating emerging trends such as acquisitions and divestitures, new accounting standards and advancements in technology. While organizations are quick to evaluate these issues for the business overall, often the internal control implications are overlooked, leading to unaddressed financial reporting risks and deficiencies.

Q: Have the following events occurred in the past three years? If so, did these events result in increased control deficiencies?

Chart data:
- Divestitures: 37% (event occurred), 9% (increased control deficiencies)
- Merger(s) and/or acquisitions: 67% (event occurred), 39% (increased control deficiencies)
- Newly adopted accounting standards: 87% (event occurred), 23% (increased control deficiencies)
- Newly implemented ERP: 37% (event occurred), 37% (increased control deficiencies)
- Rotation in external auditor: 13% (event occurred), 33% (increased control deficiencies)
- Significant business transformation: 31% (event occurred), 33% (increased control deficiencies)

■ Percentage of respondents saying the event occurred in the past three years
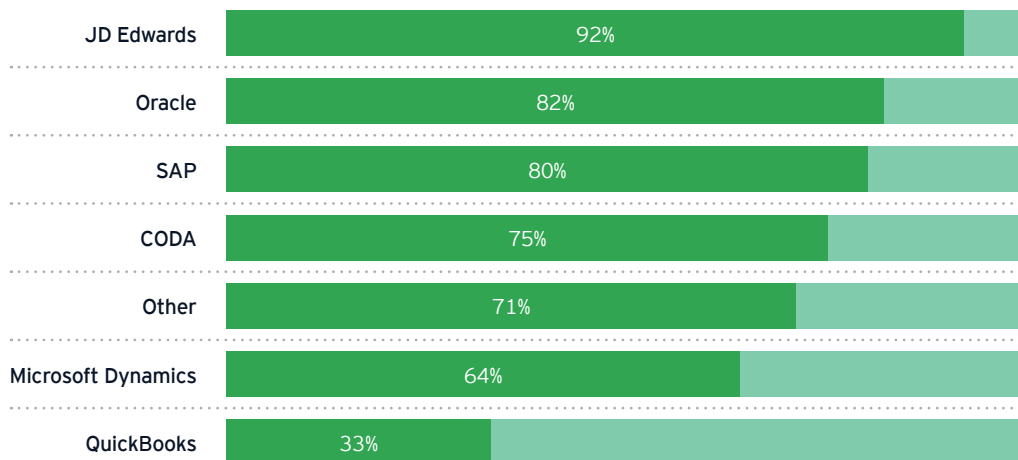■ Percentage saying this resulted in increased control deficiencies

One of the key challenges to providing effective governance and oversight is the growing complexity and scale of IT systems and environments. Organizations continue to enhance and customize their systems to match the sophistication of their business, but legacy and redundant systems are not necessarily being rationalized at the same rate. Additionally, even when organizations are utilizing large enterprise resource planning (ERP) systems, the vast majority are customized to meet specific business requirements and rule sets, making it difficult to identify all relevant controls and leverage efficiencies in testing such as the use of standard analytic scripts.

Q: What is the nature and complexity of your organization's information technology system environment? (select all that apply)

Combination of in-house developed and purchased off-the-shelf systems	72%
Utilization of large ERP	56%
Centralized	34%
Decentralized	33%
Fully customized/ developed in-house	7%

Q: Where ERPs are utilized, what is the percentage of customization?

JD Edwards	92%
Oracle	82%
SAP	80%
CODA	75%
Other	71%
Microsoft Dynamics	64%
QuickBooks	33%

In addition to keeping up with rapid emergence of new technologies, organizations also are struggling to maintain effective IT general controls (ITGCs) and completeness and accuracy of data. The survey found that, on average, ITGCs resulted in the most open deficiencies at the end of the SOX cycle; and consequently, this gives rise to more significant deficiencies and material weaknesses than any other aspect of SOX. Deficiencies in these areas were noted as the most time-consuming and resource intensive to remediate.

Moving beyond foundational governance and oversight

Progress is being made in the pursuit of increased efficiency and cost reduction. Companies are seeing other benefits to the business as a result of implementing and complying with SOX:

42%
have experienced an improved internal control environment.

28%
believe they have better risk control.

25%
have streamlined control activities.

Several of these enhancements can be traced to effective governance and program management activities, which increase management's agility to respond to changes in business and technology while reducing the level of effort to achieve compliance. Moving to an ongoing optimization process makes SOX compliance simpler yet still effective.

More than 49% of companies reassess their controls annually. Organizations are clear that reassessing helps to increase synergies and efficiencies (86%), align SOX with business risks (72%) and reduce costs (59%).
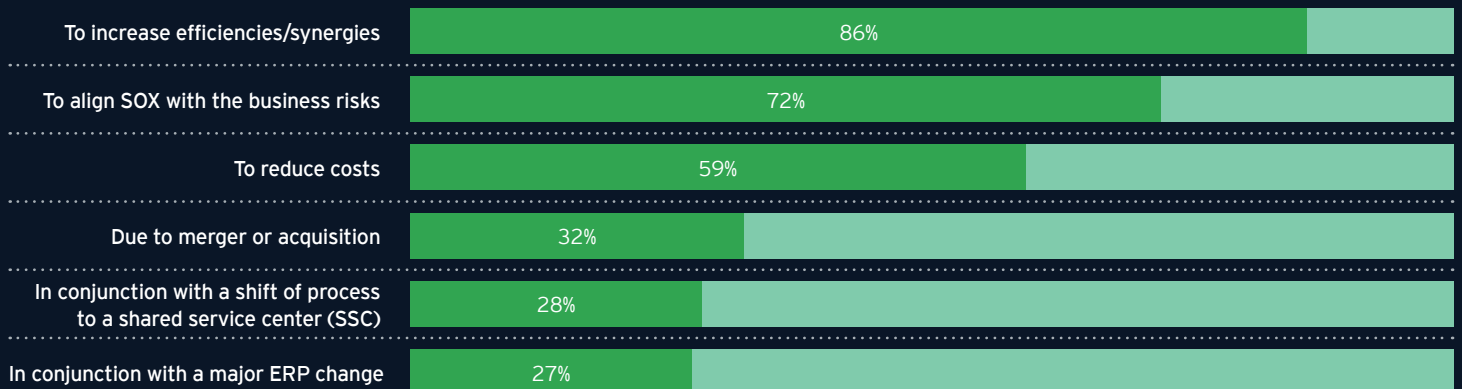
Q: Since SOX implementation, has your company taken on efforts to rationalize or optimize the internal controls structure?
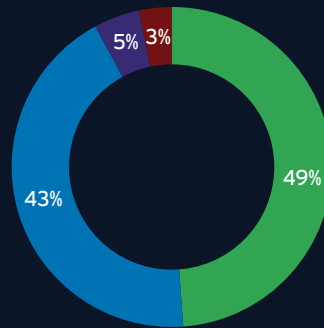
Key
- Yes, we assess annually.
- Yes, we assess as necessary.
- Yes, we assess at another frequency.
- No, we have not assessed our controls.

5% 3%
43% 49%

Q: Why did you decide to reassess or rationalize your controls?

To increase efficiencies/synergies	86%
To align SOX with the business risks	72%
To reduce costs	59%
Due to merger or acquisition	32%
In conjunction with a shift of process to a shared service center (SSC)	28%
In conjunction with a major ERP change	27%

Additionally, three out of four organizations describe their internal control activities as centralized to a reasonable extent, which demonstrates a high level of maturity in existing process and control activities. Consider harmonizing GRC functions to help reduce redundancies, consolidate controls and identify common controls.

Q: How centralized is the company's internal control activity?

Key
- Very centralized
- Centralized to a reasonable extent
- Decentralized

26% | 45% | 29%
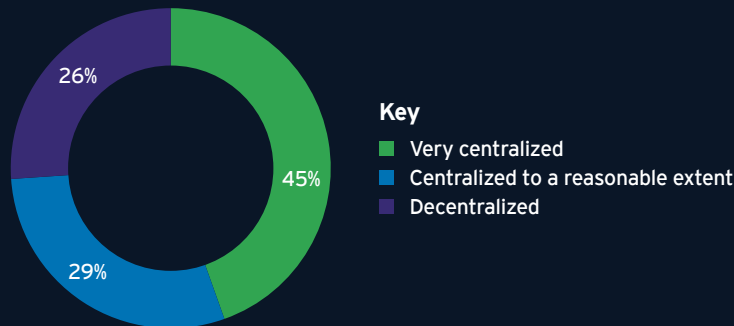
Today, significant reliance is being placed on management's testing by external auditors: 43% on IT, and 40% on business process. Consider taking a more proactive approach to scoping and planning to find the optimal balance between management's testing and external audit reliance. Challenge areas where there is little to no reliance is placed.

Q: What is the perceived percentage of reliance on management's test results by your external auditor?

IT	43%
Business process	40%

Q: Where little or no reliance is placed on management's SOX testing, which option best describes the perceived reason?

Response	Percentage
Unsure	50%
Methodology standards have not been agreed upon with the independent auditor.	22%
Real or perceived lack of competence and objectivity in management's SOX activities.	13%
Control self-assessment process not approved by independent auditor.	8%
There is a lack of formal risk assessment and scoping approach.	7%

Ways to increase reliance by the external auditors

▸ Functionally align in a manner that supports independence and objectivity in appearance and in fact

▸ Increase coordination through regularly scheduled meetings and documented meeting notes

▸ Consider development of a program playbook outlining the rules of the game, including scope, sample guidance, template(s), deficiency management, communication protocols, quality control procedures, key deliverable dates and roles and responsibilities; make sure the playbook is reviewed by relevant parties to confirm alignment with goals

▸ Consider use of external auditor's testing templates; at a minimum, share samples of completed documentation in advance for feedback

▸ Prioritize alignment on process and control documentation; note that leading practices include development of control attributes outlining (at a high level) the steps control owners take to execute key controls
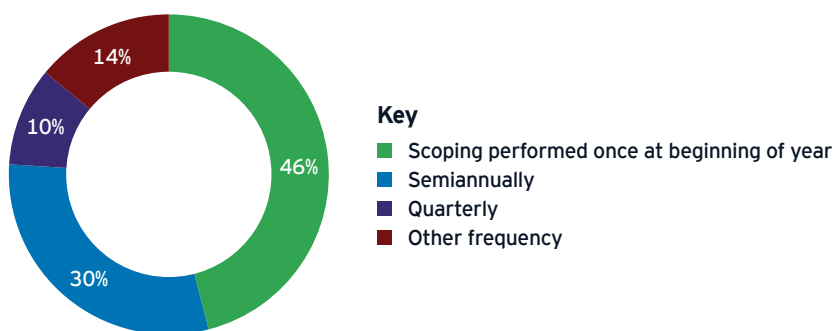
Responsive and risk-based operating model enabled by technology

Technology is an inescapable part of our lives, and while it has provided critical improvements for the business, SOX programs have been hesitant to embrace potential opportunities on a large scale. Take the scoping process as an example — 91% of organizations are using both quantitative and qualitative data to define in-scope locations and processes, but 46% look at scoping only once at the beginning of the year. Considering a data-rich world, should there be a heavier emphasis on the use of data analytics to drive ongoing scoping assessments?
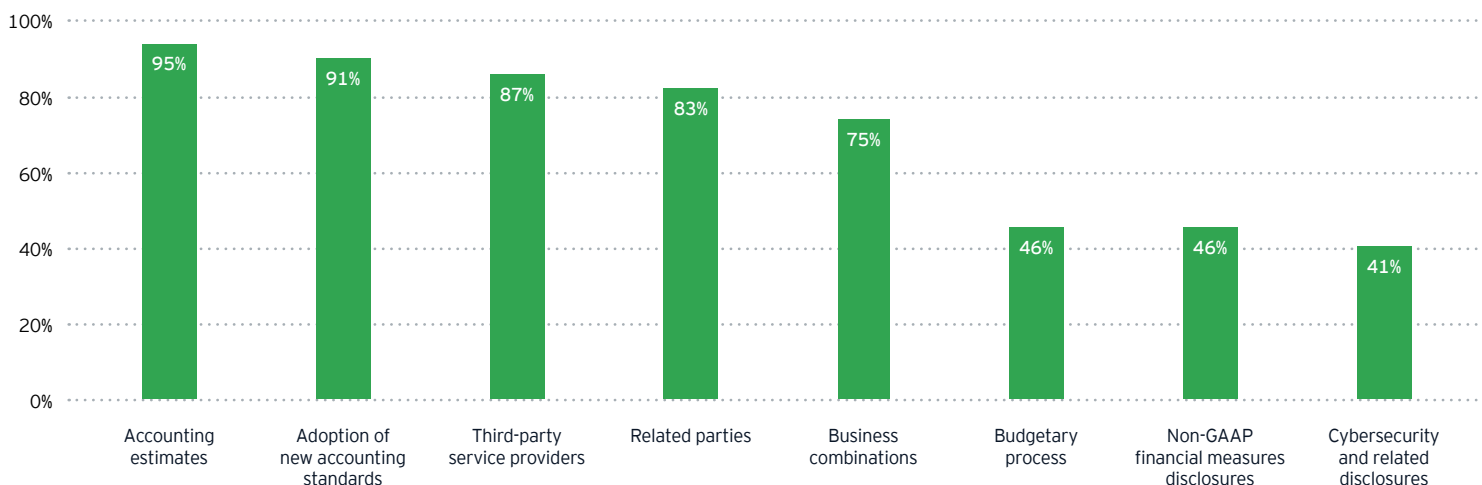
Q: How often do you refresh SOX scoping during the year?

Key
- Scoping performed once at beginning of year
- Semiannually
- Quarterly
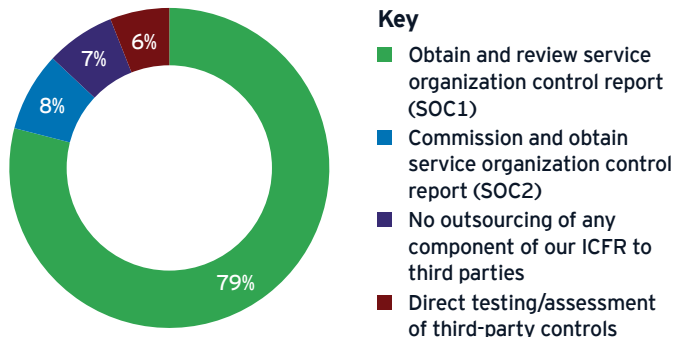- Other frequency

(14%, 10%, 46%, 30%)

How can management provide more real-time feedback to the business and key stakeholders throughout the year? Should updates to scoping and risk coverage be driven by financial cycles and significant changes to the business and technology landscape?

SOX scoping and risk assessments are just one piece of the puzzle when it comes to staying apprised of emerging business areas and new processes. More than ever, different aspects of operations, such as cybersecurity, budgetary processes and third-party service providers, are intertwined with financial risks and assertions. Leading SOX programs consider the deep implications of activities and the internal control frameworks required to manage material risk.

Q: Does your organization have SOX controls over the following emerging areas?

| Accounting estimates	Adoption of new accounting standards	Third-party service providers	Related parties	Business combinations	Budgetary process	Non-GAAP financial measures disclosures	Cybersecurity and related disclosures
95%	91%	87%	83%	75%	46%	46%	41%

Q: How does management assess the impact of services provided to third-party service organizations on internal controls over financial reporting (ICFR), including the risks of material misstatements?

Key
- Obtain and review service organization control report (SOC1) — 79%
- Commission and obtain service organization control report (SOC2) — 8%
- No outsourcing of any component of our ICFR to third parties — 7%
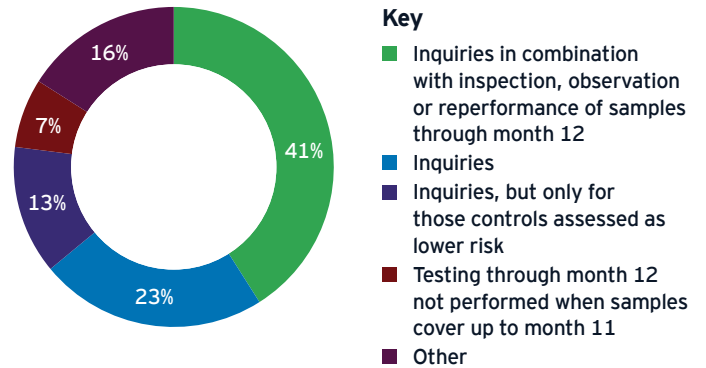- Direct testing/assessment of third-party controls — 6%

In today's environment, having a responsive operating model goes beyond just scoping and planning. SOX testing and timelines are being reinvented through technology enablement, including robotic process automation (RPA), chat bots and advanced workflow tools. Innovation can help organizations maximize coverage and efficiency, while managing the total level of effort and resources. Forty-one percent of organizations indicated SOX testing activities cover up to month 12, and 77% perform inquiries to confirm no significant changes prior to year-end.

Q: Generally, what is the period through which coverage is provided during your testing phase?

Key
- Up to month 12 — 41%
- Up to month 9 — 28%
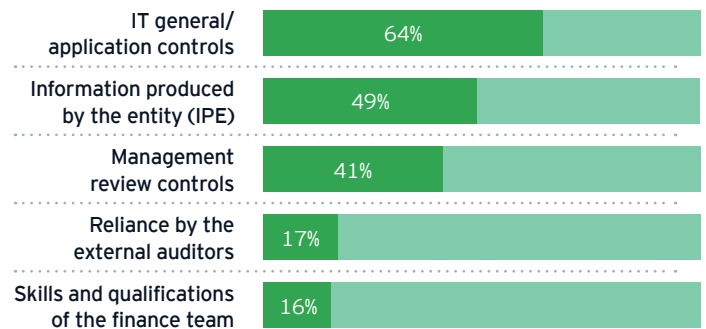- Up to month 10 — 15%
- Up to month 11 — 8%
- Other — 8%
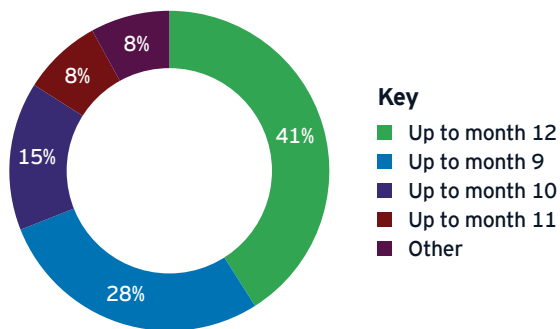
Q: If your testing period covers less than 12 months, what procedures are performed to confirm no significant changes in the key internal controls have occurred?

Key
- Inquiries in combination with inspection, observation or reperformance of samples through month 12 — 41%
- Inquiries — 23%
- Inquiries, but only for those controls assessed as lower risk — 13%
- Testing through month 12 not performed when samples cover up to month 11 — 7%
- Other — 16%

Nonetheless, organizations need to balance their appetite for risk and driving efficiencies. Several aspects of internal controls continue to challenge operational reliability and stability.

Q: In which areas are you experiencing the most challenges implementing a reliable and sustainable internal control function? (select all that apply)

- IT general/application controls — 64%
- Information produced by the entity (IPE) — 49%
- Management review controls — 41%
- Reliance by the external auditors — 17%
- Skills and qualifications of the finance team — 16%

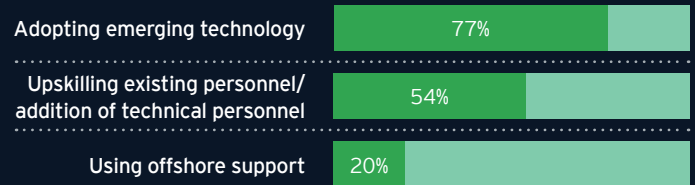# Moving beyond incremental technology enablement in SOX

The survey found that three out of four companies see the adoption of emerging technology as the leading way to transform their SOX function in the next three years, with data analytics being the most prevalent technology used in SOX today (one out of five). However, the collective adoption of emerging technology is still largely haphazard. This was the case across all company sizes and geographic regions, and respondents noted funding as the biggest barrier.
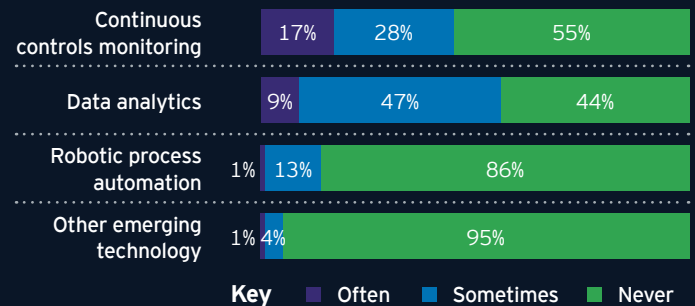

Key technology considerations

- ▸ Organizations should consider showcasing proofs of concept as evidence of increased efficiency to investment.
- ▸ By improving efficiency and doing more with less, internal controls organizations can free up resources for more value-added activities.
- ▸ Considering the internal control implications around the use of data provided by the business and the complexity and cleanliness of available data is key.
- ▸ Most technological innovation is dependent upon the availability of timely and reliable information.
- ▸ A data-driven approach may result in less investigation of non-issues, but keep in mind that initially it could uncover control exceptions never before identified.
- ▸ It is important to consider opportunities to optimize key processes through RPA and discuss the benefits with stakeholders.
- ▸ The most cost-effective bots are those that can be leveraged across multiple processes or business units.

Q: How do you see your SOX function transforming in the next three years? (select all that apply)
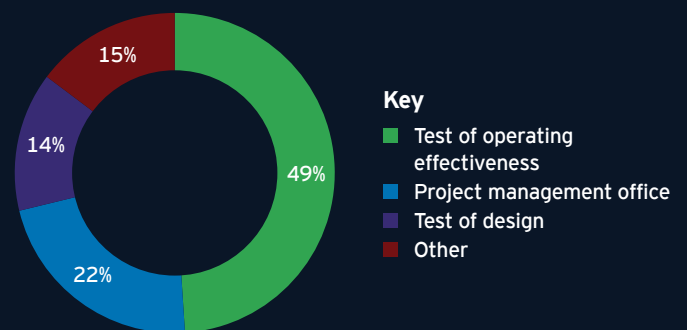
Adopting emerging technology	77%
Upskilling existing personnel/ addition of technical personnel	54%
Using offshore support	20%

Q: How often are the following used as part of the SOX assessment process?

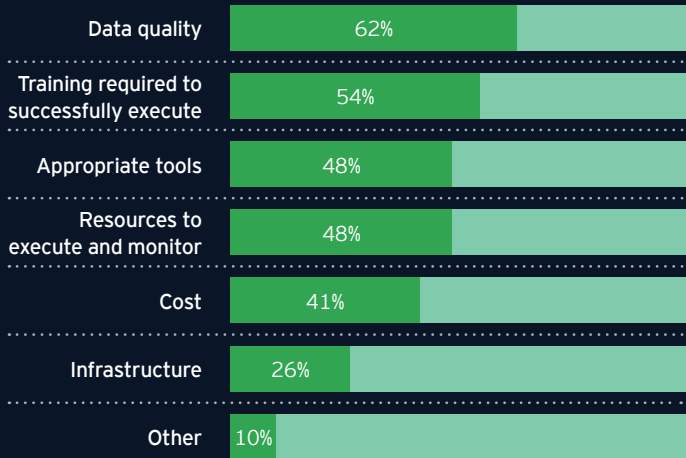|	Often	Sometimes	Never
Continuous controls monitoring	17%	28%	55%
Data analytics	9%	47%	44%
Robotic process automation	1%	13%	86%
Other emerging technology	1%	4%	95%

Key ■ Often ■ Sometimes ■ Never

Data analytics and visualization tools can provide insights and empower informed decision-making to assist with SOX scoping, planning, execution and reporting.

Q: In what areas do you use, or plan to use, data analytics as part of your SOX compliance approach?

Key
- ■ Test of operating effectiveness — 49%
- ■ Project management office — 22%
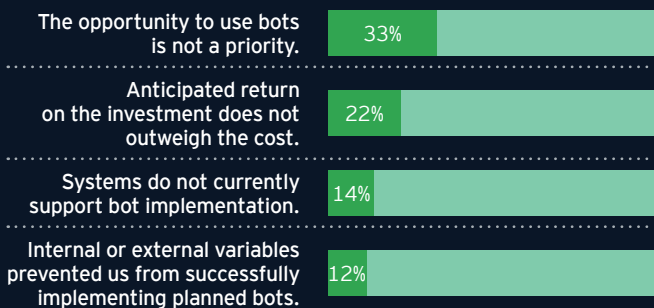- ■ Test of design — 14%
- ■ Other — 15%

The use of analytics drastically improves efficiency and can reduce costs, but significant challenges remain in the areas of data quality, such as data normalization from multiple systems. Additionally, adequate training is required to successfully deploy more robust tools within the SOX functions.

Q: In your opinion, what are the challenges of using analytics?

Data quality	62%
Training required to successfully execute	54%
Appropriate tools	48%
Resources to execute and monitor	48%
Cost	41%
Infrastructure	26%
Other	10%

On the other end of the spectrum, less than 16% of companies are utilizing RPA to execute their SOX program process. And only 30% of the companies surveyed are using RPA to perform key controls such as reconciliations, data analysis, ITGCs and key performance indicators. When RPA is being used by the business, 66% of SOX programs are testing the bots as part of their assessment.

Q: If you have not deployed robotic process automation to help you execute management's SOX assessment, what are the reasons? (select all that apply)

The opportunity to use bots is not a priority.	33%
Anticipated return on the investment does not outweigh the cost.	22%
Systems do not currently support bot implementation.	14%
Internal or external variables prevented us from successfully implementing planned bots.	12%

Continuous program improvement

As we look toward technology and automation as the future of work, we cannot overshadow the critical role people continue to play in the way we work. New technologies require new skills and, just as importantly, new ways of working. Fifty-four percent of companies agree that upskilling existing personnel or adding technical resources is key to transforming their SOX function over the next three years, which came in second to the top response of adopting emerging technology.

In the same light, organizations are focused on increasing communication and training of process and control owners to keep pace with changes happening in the business, external regulatory requirements and the overall control environment. Prioritizing training as a means to communicate and engage with the business provides an opportunity to demonstrate the benefits beyond compliance, helps keep process and control documentation current, and serves as a reminder that process and control owner actions may impact other departments and functions.
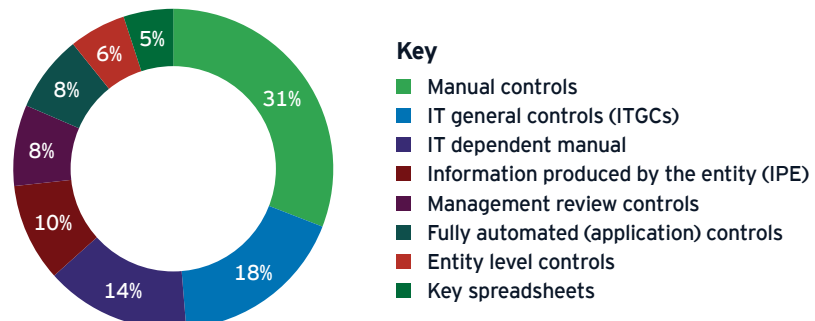
Q: How often do you perform SOX training of process/control owners?

Key
- Annually — 39%
- When there are material changes in the requirement (e.g., COSO 2013) — 35%
- Not since implementation — 7%
- Other — 19%
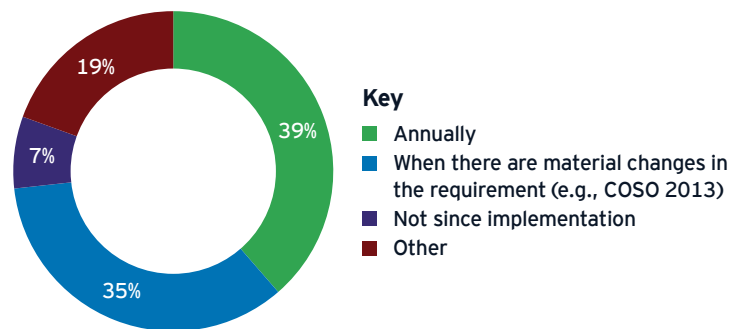
Considering the digital transformation and advancements in technology that have taken place since the inception of SOX, one would expect the look and feel of SOX to have evolved to be more autonomous and digitized. But, if you look at the foundational building blocks of SOX – process flows/narratives and controls – companies are still dependent on static, point-in-time information. It remains very difficult to implement new ways of working when controls are still largely manual and walk-throughs are not end to end.
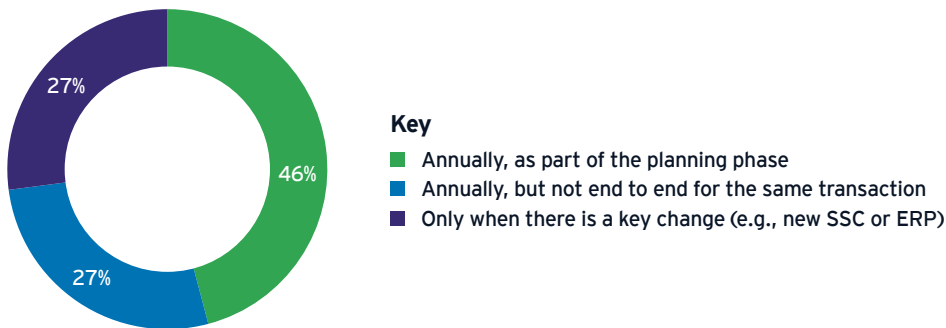
For example, respondents indicated that approximately 30% of their controls, on average, are classified as manual. Given the trends in data and technology today, are there truly manual controls that still exist where a human must physically perform a control activity without the use of a computer or other information? If controls are not in fact manual in nature, is the current test approach still relevant to cover the appropriate financial statement risk and assertions?

Q: What is the breakdown of in-scope key controls by type that are in place to support management's assessment? (average across all respondents)

Key
- Manual controls — 31%
- IT general controls (ITGCs) — 18%
- IT dependent manual — 14%
- Information produced by the entity (IPE) — 10%
- Management review controls — 8%
- Fully automated (application) controls — 8%
- Entity level controls — 6%
- Key spreadsheets — 5%

39%
of companies perform annual SOX training, and another

35%
provide training when there are material changes in the requirements for SOX.
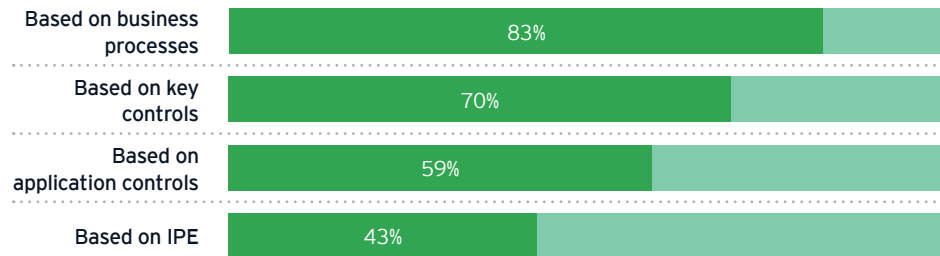
Additionally, less than half of all respondents (46%) perform end-to-end walkthroughs of a single transaction for all key processes and controls on an annual basis. And 83% said they rely on the business process as the most common source of information used to determine in-scope IT systems, which might be a factor in why deficiencies in ITGCs are still the highest, on average, across all categories and among the most difficult areas to implement reliable and sustainable controls.

Q: Do you perform end-to-end walk-throughs (e.g., tracing the same transaction from initiation to recording in the general ledger) of all of your SOX key financial processes?

Key
- ■ Annually, as part of the planning phase
- ■ Annually, but not end to end for the same transaction
- ■ Only when there is a key change (e.g., new SSC or ERP)

27%
46%
27%

Q: Which of the following are used to determine in-scope IT systems? (select all that apply)

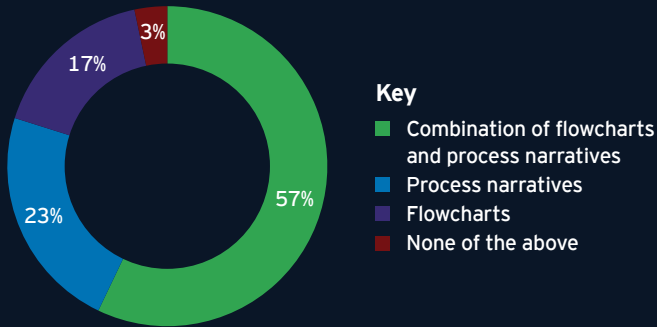|	
Based on business processes	83%
Based on key controls	70%
Based on application controls	59%
Based on IPE	43%

Companies need to continue to challenge their people and SOX programs to drive continuous improvement and change.

# Moving beyond participating to collaborating on SOX

As processes and systems continue to grow and become more complex, data flows and diagrams are becoming more critical to all stakeholders, and large-scale software developers may include capabilities to show process maps in the future. More than half of organizations surveyed are utilizing a combination of flowcharts and process narratives to capture relevant information through SOX.

Q: How are management's processes and controls documented?

- **57%** Combination of flowcharts and process narratives
- **23%** Process narratives
- **17%** Flowcharts
- **3%** None of the above

Key
- 🟩 Combination of flowcharts and process narratives
- 🟦 Process narratives
- 🟪 Flowcharts
- 🟥 None of the above

Key program improvement considerations

▶ Challenge requirements for flowcharts and narratives (How much value is provided to end users by preparing and maintaining both? How much is a preference versus a requirement?)

▶ Consider a hybrid approach – flowchart with narrative context in it or the adoption of business process modeling and process mining tool
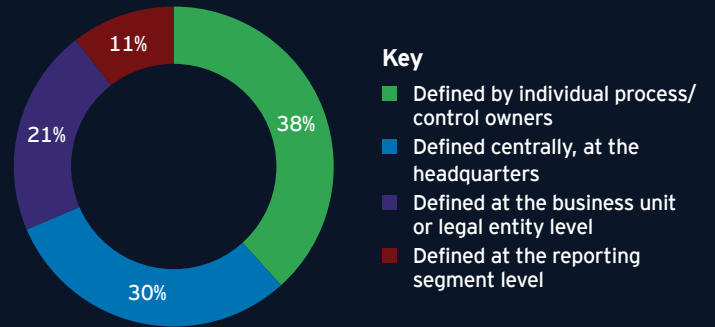
Not all aspects of process and control performance and testing will be automated. Management review controls continue to be a challenge for control owners because they cover key judgments and estimates, higher-risk transactions and higher-value financial information. Of the responses indicating the presence of a material weakness, 30% were attributed to inadequate manual review controls or deficiencies related to existing review controls.

Q: Have thresholds been designed for review controls?

- **82%** Yes
- **18%** No

Key
- 🟩 Yes
- 🟦 No
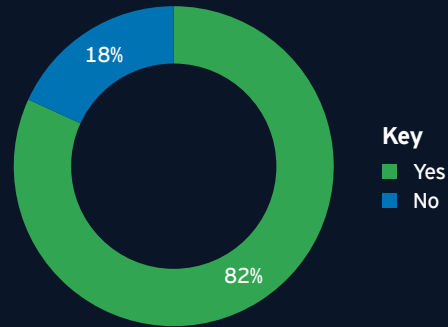
Q: Given that thresholds have been designed, at what level were precision levels defined?

- **38%** Defined by individual process/control owners
- **30%** Defined centrally, at the headquarters
- **21%** Defined at the business unit or legal entity level
- **11%** Defined at the reporting segment level

Key
- 🟩 Defined by individual process/control owners
- 🟦 Defined centrally, at the headquarters
- 🟪 Defined at the business unit or legal entity level
- 🟥 Defined at the reporting segment level

It is important to consider whether control owners understand the purpose of the review control, the risk(s) being mitigated and the extent of documentation required to evidence control performance.

Another key question is whether the appropriate thresholds have been designed and documented for review controls.

Conclusion

If we do not transform our SOX programs to keep pace with the business, this will remain a compliance exercise and fail to unlock the value the business deserves. Picture this scenario — we select a sample of 25 invoices for testing and find that one was not approved according to policy. We take that exception to the business owner and, while they agree it is an issue, they are not concerned. How can that be? As we continue to discuss the single sample, they bring up a live dashboard used to monitor exceptions on a real-time basis. Of the 100,000 invoices processed by their function to date, they can pinpoint the sample we happened to select — along with four other examples of late approval. They can also provide evidence of follow-up on these samples to obtain the appropriate approval and provide coaching to the control owner. In this case, we must ask ourselves a couple of questions: how can it be that we are still testing a sample of 25 invoices when the business is monitoring 100% of its transactions? Are we even testing the right controls? If the business is that far ahead of us, how can we add value?

This is a simple example to highlight a complex issue. It is certainly not easy to transform an existing program overnight and, with disruption happening on an almost continuous basis, it is easy to be bogged down in the current state. But, it has to be done to maintain, build or rebuild trust within the organization. Transforming your SOX program is not a one-time, big-bang exercise, but an ongoing opportunity to do better and be better. The road map will not be the same for every function, but it is important to have a formal plan with targeted goals and action plans. While SOX may be, by definition, a compliance exercise, the benefits of an effective program can be wide-reaching.

What can you do today to catch up to tomorrow?

▸ **Evolve your operating model:** keep pace with the changes in your organization through a flexible and dynamic approach to managing and evaluating internal controls

▸ **Explore new ways to innovate through technology:** consider enhancing automated capabilities across all aspects of SOX, such as digital risk assessments, automated scoping tools and analytic testing procedures

▸ **Upskill your workforce:** look for new opportunities to cross-train on business processes and ITGCs; refresh control owner training and feedback processes

▸ **Build trust with the business:** ask for feedback on the SOX program; consider using an impartial third party (internal or external) to gather feedback; develop a plan and take action

▸ **Challenge the nature, timing and extent of testing:** ask whether you are doing too much in any area or not enough in another; determine whether control classifications are accurate and aligned to the appropriate risks (manual vs. automated)

▸ **Consider a facilitated visioning session:** focus on governance structure, operating model, talent pool, use of technology and strategy

Contacts

For assistance or more information, please contact:

Amy Brachio
EY Global Advisory Risk and PI Leader
Ernst & Young LLP
+1 612 371 8537
amy.brachio@ey.com

Esi Akinosho
EY Global Advisory Internal Audit Leader
Ernst & Young LLP
+1 713 750 8670
esi.akinosho@ey.com

Lisa Hartkopf
EY Americas Internal Audit Leader
Ernst & Young LLP
+1 312 879 2226
lisa.hartkopf@ey.com

Martin Wiedemann
EY EMEIA Internal Audit Leader
*Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft*
+49 761 1508 27466
martin.wiedemann@de.ey.com

Julia Langdon
EY Asia-Pacific Internal Audit Leader
Ernst & Young (Australia)
+61 3 8650 7289
julia.langdon@au.ey.com

Contributors

Greg Alperin	Ruchi Ruchi
Preston Jenkins	John Theisen
Neil Mathur	Kendy Thompson
Stuart Reid	

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

ey.com