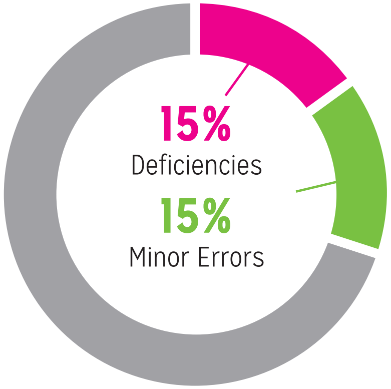
:RESOLVER

DEVELOPING A TOP-DOWN, RISK-BASED APPROACH TO SOX

DEVELOPING A TOP-DOWN, RISK-BASED APPROACH TO SOX



At its simplest, a "top-down, risk-based" approach to financial reporting is about exposure to risk related to a single objective – filing statements that are free of material error or omission.

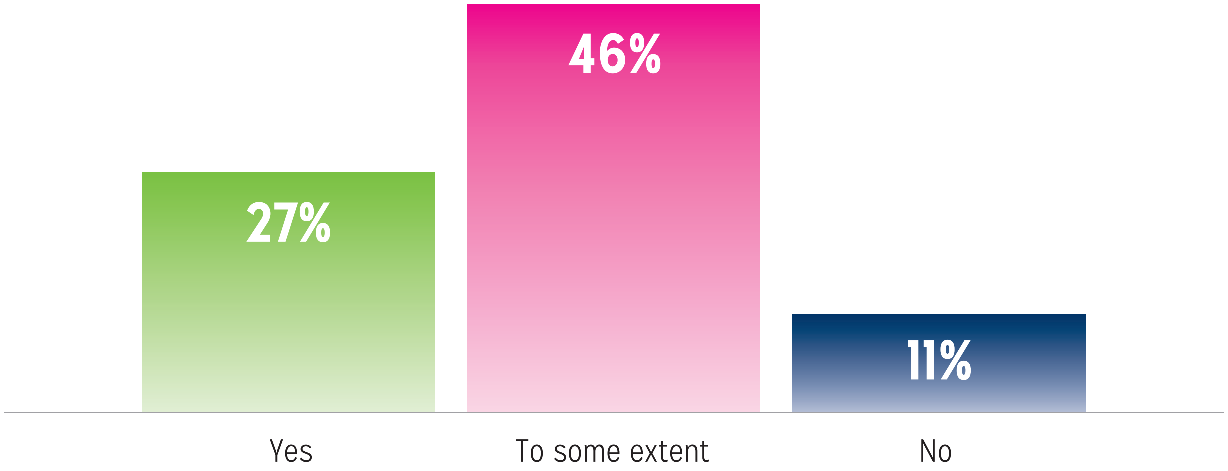
And while they're not a rampant problem, errors and omissions are still a troubling issue. PCAOB findings suggest deficiencies in audits of internal control in as much as 15 percent of audit engagements it inspects, and—in addition—relatively minor errors in an equal amount.

Deficiencies noted include failures to:

- Identify and test controls intended to address the risks of material misstatement.
- Test the design and effectiveness of management review controls.
- Obtain evidence needed to update test results on controls in the roll-forward period.
- Test controls on data and reports that themselves support other important controls.
- Sufficiently evaluate control deficiencies.

A top-down, risk-based approach—properly implemented—can mitigate the risk of these failures and more.

ARE YOU SATISFIED THAT YOU HAVE AN EFFECTIVE TOP-DOWN AND RISK-BASED SCOPE FOR SOX?



Source: Poll of 150 webinar attendees, How to develop a top-down, risk-based approach to SOX—truly, June 30, 2015.

WHAT IS TOP-DOWN, RISK-BASED… EXACTLY?

PCAOB's Auditing Standard No. 5 neatly defines the top-down, risk-based approach:

> *A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to internal control over financial reporting. The auditor then focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions. This approach directs the auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the financial statements and related disclosures. The auditor then verifies his or her understanding of the risks in the company's processes and selects for testing those controls that sufficiently address the assessed risk of misstatement to each relevant assertion.*

In a recent webinar entitled "How to develop a top-down, risk-based approach to SOX—truly", internal audit, risk management, and governance expert Norman Marks clarified that top-down is about learning to live with acceptable risks.

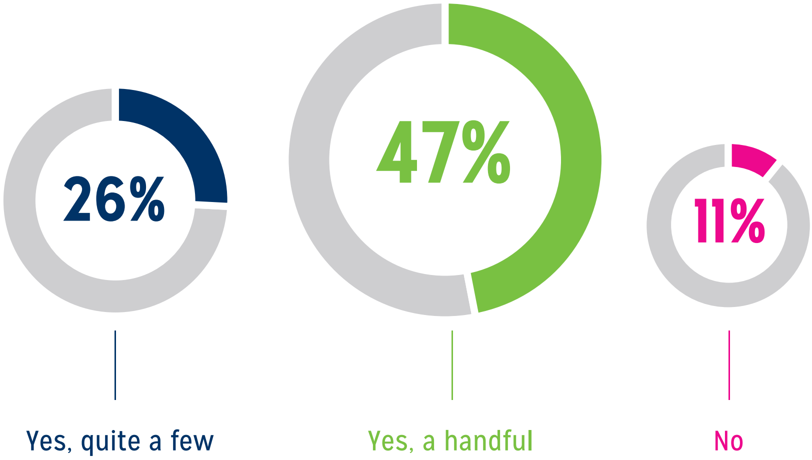
"What is the risk? Where is the risk? You need to, at all times, ensure that your scope is focused on those two questions," Marks said. "That prevents scope creep—and keeps you from getting distracted by things that would never have resulted in a material error or omission."

Success, then, lies in concentrating on areas where there is some appreciable chance of a material error or omission—and using controls to provide assurance that other risks are less than reasonably possible.

Forcus on these two questions to prevent scope creep

1. What is the risk?
2. Where is the risk?

DO YOU HAVE CONTROLS IN YOUR SCOPE THAT, IF THEY FAILED, WOULD NEVER RESULT IN A MATERIAL WEAKNESS?



Source: Poll of 150 webinar attendees, How to develop a top-down, risk-based approach to SOX—truly, June 30, 2015.

GETTING STARTED WITH TOP-DOWN, RISK-BASED

Wondering where to begin? AS5 suggests starting, predictably, at the start:

> *The auditor must test those entity-level controls that are important to the auditor's conclusion about whether the company has effective internal control over financial reporting.*

William J Powers, PCAOB National Associate Director, Division of Registration and Inspections, agrees. Powers, in the same SOX webinar, advised beginning at the financial statement level—and focusing primarily on entity-level controls and relevant assertions.

Here's what counts as an entity-level control according to AS5:

- Controls related to the control environment;
- Controls over management override;
- The company's risk assessment process;
- Centralized processing and controls, including shared service environments;
- Controls to monitor results of operations;
- Controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs;
- Controls over the period-end financial reporting process; and
- Policies that address significant business control and risk management practices.

The "mileage" you'll achieve from entity-level controls can vary, naturally. Some controls are important but only contribute indirectly to your ability to detect or prevent a material misstatement. Some do, in fact, directly influence that ability, but without the level of precision that would allow you to cut back on testing other controls.

But others, however, will do a more than adequate job of helping you prevent or detect misstatements to one or more relevant assertions.

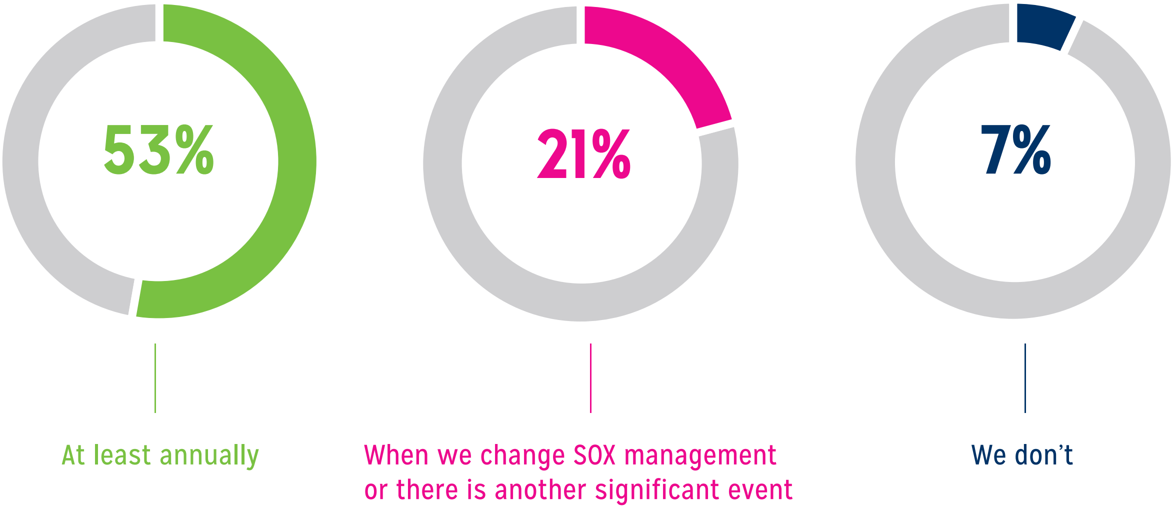
By appropriately allocating the energy you spend on these three types of controls, Powers says you'll enjoy the efficiency advantages of a top-down risk-based approach.

"Look at entity-level controls. If they can be tested and shown to be both operating and designed effectively, you can minimize the amount of testing you have to do at the process or transaction level."

Begin Here

Start

HOW OFTEN DO YOU RE-EVALUATE AND ADJUST YOUR SOX SCOPE?



Source: Poll of 150 webinar attendees, How to develop a top-down, risk-based approach to SOX—truly, June 30, 2015.

PUTTING TOP-DOWN, RISK-BASED INTO ACTION

Also speaking on the SOX webinar panel was Richard Arthurs, VP of Risk Management and Chief Audit Executive at Altalink, one of Canada's largest power transmission companies.

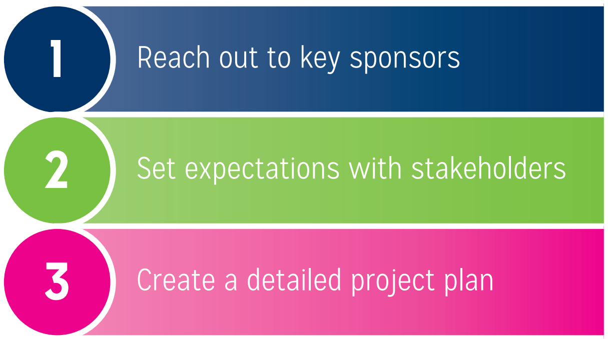
Arthurs gave tips on how to implement a top-down, risk based approach.

- Reach out to key sponsors and partners – including the CFO, Controller, Audit Committee and control owners—to ensure success. The investment you make in relationships, Arthurs said, will always pay dividends over time.
- Set expectations with stakeholders that top-down, risk-based means a reduced number of controls. Don't assume that leadership will find the value on their own; make it explicit and they'll more readily embrace your efforts.
- Create a detailed project plan with clear accountabilities. SOX isn't "one size fits all," as Arthurs pointed out, so it will be important to make sure you're doing the work that matters to your company.

Top-down, risk-based may seem daunting at first, but the benefits speak for themselves:

- An overall reduction in key controls. Arthurs has seen decreases of as much 30% or more in SOX projects with which he's been involved.
- An increased reliance on entity-level controls and automated IT general controls, leading to a significant reduction in IA resource time.
- Significant efficiencies—especially if you plan on using governance, risk and compliance software to visualize and report on your efforts.

Implementing a top-down, risk based approach

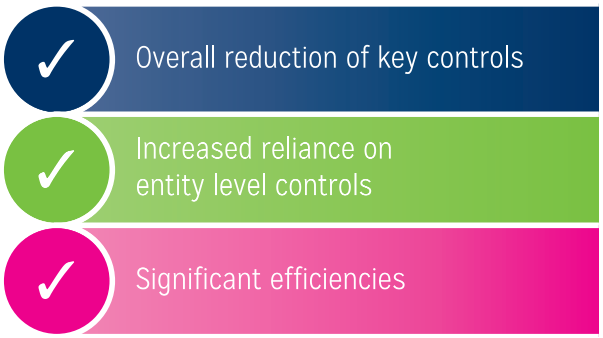


1 Reach out to key sponsors

2 Set expectations with stakeholders

3 Create a detailed project plan

Benefits



✓ Overall reduction of key controls

✓ Increased reliance on entity level controls

✓ Significant efficiencies

INTERESTED IN LEARNING MORE?

WEBINAR

How to develop a top-down, risk-based approach to SOX—truly

Where there is at least a reasonable possibility of a material error or omission, you have a financial reporting risk that must be addressed.

A top-down risk-based approach to that risk frees you to reduce your efforts where it's less than reasonably likely that a material error or omission could occur, and lets you focus instead on high-impact issues of internal control.

If you'd like to learn more, you may be interested in "How to develop a top-down, risk-based approach to SOX—truly", the webinar from which some of the material in this paper was drawn.

The webinar, sponsored by Resolver, is available for free viewing by clicking the link on the left (in blue).

ABOUT RESOLVER:

Resolver is the risk backbone for over 1000 of the world's largest organizations. Our governance, risk and compliance software takes the uncertainty from Decision-Making, Internal Control, Internal Audit, Compliance Management, Enterprise Risk Management and Incident Management. Resolver's team is comprised of risk, compliance, and security experts supporting customers across 100 countries with offices in North America, United Kingdom, and the Middle East.

If you'd like to learn more about GRC software for SOX compliance from Resolver, watch a guided tour or request a demo.

:RESOLVER

888.891.5500 | RESOLVER.COM