

6 Steps to Performing Your SOX Risk Assessment



As we begin to close out a new year, the most important part of your SOX program that needs to be re-evaluated and updated is the SOX risk assessment.

The SOX risk assessment, if not performed correctly, could result in unnecessary work for your team, management and external auditors, leading to over-worked team members and excessive costs. Worse, your organization could have insufficient or incorrect controls in place to prevent or preemptively detect a material misstatement.

Internal auditors with a solid understanding of how to conduct a SOX risk assessment, what is material and why controls are key, are extremely valuable to their CFO and executive management. These individuals will be more influential and credible when working with the external auditors in negotiating

whether new controls should be added, if extra documentation is needed for evidence or how control observations should be extrapolated.

For some of us, the SOX risk assessment may be a new endeavor. Maybe you've recently started at a new company and inherited a risk assessment, or maybe there haven't been enough changes in people, process and technology to warrant performing or re-performing this key task.

Whatever the reason, we've provided risk assessment guidelines that can help. By following these six steps, any internal auditor or controls expert should be able to carry out a preliminary SOX risk assessment. Chances are, you'll be helping your company's financial reporting control environment or saving company resources with your ability to have a more informed conversation with your external auditor.

STEP

1

Determine what is considered material to the P&L and balance sheet.

How: This is usually determined by calculating a certain percentage of key financial statement accounts. For example, 5% of total assets, 3-5% of operating income, or some analysis of multiple key P&L and BS accounts. It's good to check with your CFO and external auditor to get their thoughts on this.

STEP

2

Determine all locations with material account balances.

How: Analyze the financials for all of the locations you do business in. If any of the financial statement account balances at these locations exceed what was determined as material (in *Step 1*), chances are they will be considered material and in-scope for SOX in the coming year.

STEP

3

Identify transactions populating material account balances.

How: Meet with your controller and the specific process owners to determine the transactions (*i.e. debits and credits*) that cause the financial statement account to increase or decrease. How these transactions occur and how they're recorded should be documented in a narrative, flowchart or both.

STEP

4

Identify financial reporting risks for material accounts.

How: Seek to understand what could prevent the transaction from being correctly recorded, or the risk event. Then, document the effect the risk event could have on how the account balance could be incorrectly recorded, or the breakdown of the financial statement assertion.

STEP

5

Identify and document controls preventing or detecting transactions from being incorrectly recorded.

How: Seek to identify the checks and balances in the financial reporting process that ensure the transactions are recorded correctly and account balances are calculated accurately.

Some examples of preventative or detective controls include segregating conflicting duties (*e.g. the ability to post and approve invoices*), reviews of individual or multiple transactions recorded in the period, and account reconciliations.

STEP

6

Determine key controls.

How: Of all the controls identified in *Step 5*, determine which ones, either individually or in aggregate, if operating effectively, would provide reasonable assurance that the transactions populating the material account balance will be recorded correctly. Material accounts usually, but not always, need multiple controls in place to prevent a material misstatement from occurring. You'll have to analyze all of the controls to determine which ones best provide that assurance, keeping in mind the people, process and technology in place.

These six steps will significantly help someone who has never performed a SOX risk assessment before. The PCAOB's Auditing Standard #2201 and Normal Mark's book are also good resources, and AuditBoard's team of experienced SOX and internal controls professionals can also be of assistance.

