

# SOX Compliance: 10 Steps to Savings

When George W. Bush signed the Sarbanes-Oxley Act (SOX) in 2002, he said it included “the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt.”<sup>1</sup> Today, opinions are divided about the impact SOX has had on cleaning up corporate fraud and restoring confidence in the public markets. Furthermore, though compliance costs have declined, they are still significant. A 2007 study conducted by Financial Executives International (FEI) put average corporate compliance costs at \$1.7 million.<sup>2</sup> Thus, it’s not surprising that many public companies believe the costs of SOX compliance outweigh the benefits—especially in these turbulent economic times. With careful planning and preparation however, public companies can turn SOX compliance into a business advantage, while saving money and time in the process.

## Planning Ahead

Regardless of how much time companies can allocate to SOX 404 compliance, they will save money by planning ahead. While some public companies are able to spread their compliance efforts out over the year, many still incur much of the work during third and fourth quarters. In these cases, the best time to begin planning for SOX testing is in the second quarter. That means *right now* for calendar-year companies. This leaves third and fourth quarters to testing, fixes and re-testing, and first quarter next year to completing financial reporting testing.

Randy Choi, corporate controller at Tektronix Inc., explains, “Effective upfront planning allows for potential audit issues to be identified sooner. This, in effect, helps minimize the number of surprises management may encounter toward the end of the project.”

Since accelerated filers have complied with SOX at least five times and non-accelerated filers have complied with Section 404 (a) once, the following 10 steps are appropriate for companies that have experience with SOX, Section 404.

---

<sup>1</sup> Bumiller, Elisabeth, “Bush Signs Bill Aimed at Fraud in Corporations,” *The New York Times* (July 31, 2002).

<sup>2</sup> Annual FEI survey of 168 accelerated filers with average revenues of \$4.7 billion. Figures mostly due to labor and costs associated with SOX, Section 404. (2007)

## **Step 1: Validating the Process List**

The first step in planning a SOX compliance project is to ensure that the right business processes are included in scope. The challenge here is to focus only on activities that are essential to financial reporting. That means excluding COSO objectives related to operations, laws and non-financial regulations. If it's unclear what is in scope, it's helpful to consider whether it relates to ensuring correct financial reporting, evaluating management's authorization of transactions or safeguarding assets. By refining the scope, a company lays the foundation for a compliance project that is easier for them—and their auditors—to manage.

When evaluating business processes, it's important to keep materiality threshold in mind. When the dollars flowing through those processes exceed the threshold, they should be included in the scope of the SOX project. Most companies accomplish this by mapping their processes to the general ledger. As today's economy impacts balance sheets and income statements, certain business processes need to be reevaluated for inclusion or exclusion. Further, companies should adjust their overall materiality thresholds, as the factors used to calculate those thresholds have probably changed too. Some specific processes to reexamine for inclusion or exclusion include:

- Capturing and recording accruals
- Non-operating income
- Non-operating expense
- Asset acquisition, delivery and set-up
- Internally developed assets
- Asset impairment
- Asset disposal
- Hiring and termination
- Travel and entertainment
- Vacation and payroll accruals
- Bad debt allowance
- Sales and purchases of investments

## Step 2: Leveraging COSO Small Business Guidance

Many officers at small public companies argue that SOX treats small businesses unfairly.

Although they have lower dollar profits than their larger counterparts, they still have the same number of processes to document and test. COSO's response to this comes in their manual, Guidance for Smaller Public Companies (COSO's 2006 Guidance).

Companies of all almost every size will find the information and checklists in this manual useful in streamlining their process and testing documents and cutting down on testing time.



Readers will find Volume III, Section VII particularly valuable, as it contains guidance on information technology controls for less complex IT environments. Companies that rely on manual controls for system outputs, use off-the-shelf software, have centralized processing with few interfaces, employ simple spreadsheets or outsource IT functions will find ways to reduce SOX compliance effort by adopting the simplified guidance in this section.

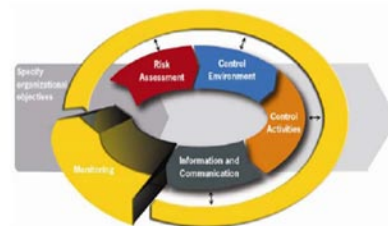
## Step 3: Using Indirect Monitoring to Reduce Direct Testing

In January 2009, COSO published the Guidance on Monitoring Internal Control Systems (COSO's 2009 Guidance). Like COSO's 2006 Guidance referenced above, this publication is a must-read for SOX project managers. Although the scope of COSO extends beyond SOX financial reporting, this three-volume publication provides examples and checklists that can be directly applied to a SOX project. It guides readers through using the monitoring they already have in place, rather than recommending they create new and redundant controls.

The COSO model takes monitoring beyond testing of controls to include monitoring the risks, control environment, the controls themselves and information (see old and new monitoring model). It also



**Old monitoring model**



**New monitoring model**

explains the concepts of direct and indirect information and ongoing and separate monitoring:

- **Direct information** refers to testing the control itself.
- **Indirect information** refers to information about a control's operation, which can be used to justify less intense direct testing.
- **Ongoing monitoring, or built-in controls**, allows testers to identify deficiencies faster, reducing the need for separate monitoring and additional testing. Examples include supervisory activities, peer comparisons, trends, reconciliations and continuous monitoring using software utilities.
- **Separate monitoring, or add-on controls**, provides independent testers with objective feedback on controls and insight into how ongoing monitoring is working.

By using the right balance of information and monitoring, a company can watch a process or specific risk more effectively and reduce the need for add-on testing.

COSO's 2009 Guidance, Volume III contains 46 real-world monitoring examples. SOX project managers should review this information for ideas about how to save time by implementing monitoring on their own projects.

#### **Step 4: Sub-Certifying and Asking About Changes**

Before beginning a new SOX testing cycle, it's crucial to ensure that any deficiencies identified in the prior year have been resolved. This can be a big task. The most effective way to solve a control deficiency is to enlist the process owner's help. The process owner is already familiar with the process and ideally positioned to help devise a solution.

The SOX team should use a deficiency evaluation form to provide input and direction to the process owner. The most effective form has four sections:

1. **The tester's explanation of the deficiency**
2. **A SOX manager's evaluation and recommendation**

3. **The process owner's remediation:** The process owner may choose to implement the SOX team's recommendation or devise another solution. Upon proposing a solution, the process owner sends the form back to the SOX project manager.
4. **The SOX team's evaluation and approval**

The SOX project manager should ensure that process owners have resolved all prior-year deficiencies listed in the evaluation forms, unless the company decides that the underlying risk cannot justify the remediation costs.

While the process owner should mitigate known deficiencies, the SOX project manager should also make sure that processes haven't changed from the prior year and that the controls are still operating (i.e., well designed, passed testing in the prior year or remediated in the current year). This is best accomplished with a confirmation from each process owner, also known as a sub-certification or management representation. COSO's 2009 Guidance, Appendix B has an excellent, seven-page management representation that any company could adapt for its use. Ideally, this representation should be sent to the process owners in the second quarter and returned before testing begins in the third quarter.

According to Shawn Bargouti, senior manager of Internal Controls at InFocus Corporation, "Coordinating and setting expectations with process owners prior to beginning the documentation and testing phase will save the entity significant time and resources."

### **Step 5: Negotiating SAS 70**

Companies should obtain SAS 70 audits from third-party outsource vendors whose actions may impact their financial reporting. These audits are expensive, often costing hundreds of thousands of dollars or more. Since many third-party outsource vendors do not want to cover the costs of these audits and older contracts do not address SAS 70, the outsource vendors will attempt to pass the costs on to their clients (i.e., the company). Paying for a SAS 70 can increase a SOX project budget significantly. To avoid this, a company should ensure its contract with an outsourced provider specifies that they will obtain and pay for a SAS 70 audit when necessary.

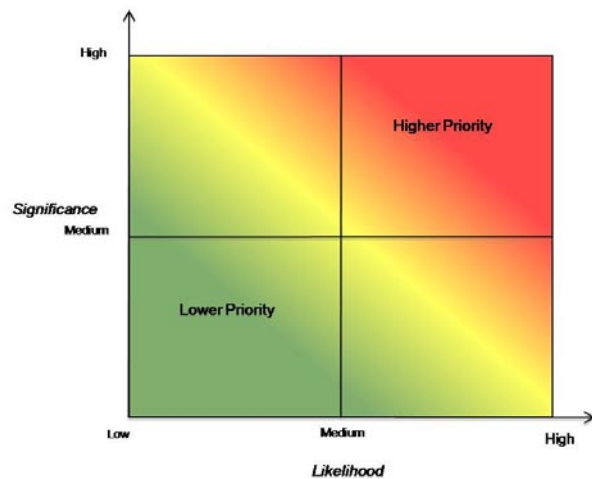
It's a good idea to start these negotiations early and involve the company's procurement department in case the outsource contract needs amending.

### Step 6: Performing Risk Assessment

Most SOX teams are familiar with the term "risk-based approach." In a risk-based audit, the auditor's testing of controls and testing of accounts and disclosures are directed toward the areas of greatest risk. The risk-based audit approach was first discussed for SOX in the May 2005 PCAOB guidance. This was formalized when Auditing Standard #5 (AS#5) was approved in July 2007. The SEC released similar guidance directed at public companies in June 2007.

Mr. Bargouti, describing the relationship between planning and risk identification says, "Significant savings can be had with proper planning. Planning starts with management identifying the entity's key financial risks and evaluating the likelihood and significance of those risks."

SOX teams should evaluate risk in 2009 and leverage their risk analysis, if any, from 2007 and 2008. By identifying risk factors and grading every business process and control, SOX teams can adjust their compliance testing. SOX Teams may use a 'Heat Sheet' to illustrate this visually. This can help the business realize real savings without sacrificing project quality.



Space does not permit listing all risk factors here, but readers can refer to the SEC guidance for process and control risks factors in Commission (SEC) Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, pages 25-27.

COSO's 2009 Guidance also provides a list of risk factors and their specific effects on monitoring as an outcome. These include:

- Direct versus indirect monitoring (Volume II, Application, paragraph #76)
- Sufficiency of information gathered for monitoring (Volume II, Application, paragraph #82)

Fortunately, COSO's risk factors are quite similar to the SEC's. Readers may wish to read about these COSO factors too and substitute or supplement the SEC's recommended risk factors.

Additionally, readers will find a handy Microsoft® Excel® tool containing both SEC and COSO risk factors on the Cost Advisors website. It can be downloaded for free at [www.costadvisors.com](http://www.costadvisors.com) or from the OSPCA website at [www.needlink.com](http://www.needlink.com).

Using risk rating, a company can adjust its testing and monitoring in the following ways:

- Varying testing procedures: inspection, observation, inquiry, confirmation, recalculation, re-performance or analytical procedures
- Varying sample sizes
- Varying sampling frequency (timing of testing)
- Altering who performs the monitoring (testing): self, peer, supervisor, impartial employee auditor or independent consultant
- Varying the type of monitoring information collected (direct versus indirect)



Step 8 addresses the external auditor's considerations when making decisions about adjusting testing and monitoring.

### **Step 7: Deciding Key Controls**

Considering key controls is a logical next step, because the type of control that is needed can vary based on the process risk assessment. If new key controls are identified here, the SOX team should reassess their risk of failure, as discussed in Step 6. Additionally, the presence of

monitoring (Step 3), extent of sub-certification (Step 4) and the availability of a SAS 70 (Step 5) may also affect key control identification.

For efficiency's sake, fewer—but stronger—key controls mean less testing year after year.

Additional factors to consider when identifying key controls are:

- The control must be working and there must be some evidence of this.
- The control must be sensitive enough to prevent or detect the risk (error), or else the control must ensure that other controls are working.
- The control should be easy to test. (For example, IT controls are usually easy to test.)
- The control mitigates many risks.

COSO's 2009 Guidance provides the following official criteria to consider when identifying key controls:

- Their failure could materially affect the objectives for which the evaluator is responsible, but might not be detected in a timely manner by other controls.
- Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization's objectives.

Regardless of the criteria used in identifying a key control, it's important that the list be tight and efficient. Having excess, duplicate key controls that must be documented, evaluated, confirmed, monitored and tested each year is expensive, time consuming and inconsistent with the new COSO Guidance.

### **Step 8: Verifying External Auditor Reliance**

By coordinating SOX planning with external auditors, companies can often obtain auditors' reliance on work performed internally. The result: the external auditors have less original work to do and companies may save time and money on external audits if negotiated early.

Several variables affecting the external auditor's reliance are:

1. **The testers' competence:** To verify the testers' competence, the external auditor will want to see experience with SOX testing or auditing on the testers' resumes. Additionally, the testers should have credentials that indicate their familiarity with business processes, including certification as a CPA, Certified Internal Auditor (CIA) or Certified Management Accountant (CMA).
2. **The tester's independence:** Because a SOX project involves many controls performed by the finance and accounting departments, auditors fear that testers who report directly to finance or accounting management could suppress a control deficiency. Companies can improve reliance by having an independent channel through which the SOX team reports to the audit committee.
3. **The entity-level risk and control environment:** The top-down approach popularized by AS#5 directs the external auditor to evaluate the control environment and entity-level risk. If the entity-level controls are in shape and well documented, a company is more likely to obtain greater reliance from the external auditor.
4. **The persuasiveness of the information or evidence gathered:** Steps 3 and 6 covered the persuasiveness of the evidence gathered. Obviously, the more sufficient, reliable and timely the evidence, the more reliance the company can expect from its auditors.
5. **The timeliness and quality of the work produced:** It is very important to have neat, well-organized workpapers that have been independently reviewed by a senior manager. Workpapers with written conclusions, initials and references that closely approximate the external auditors' other workpapers are most likely to be accepted. In short, internal SOX work must be done as if it were an actual (attest) audit.

Before testing begins, the SOX project manager should review all the points above and the company's own risk assessment with the external auditor (Step 6).

### **Step 9: Hiring a Librarian**

For large SOX projects with hundreds of controls and multiple locations, a temporary librarian can be a cost-effective investment. Instead of relying completely on more expensive project

management staff, a company can have a librarian track and organize details that are important to project integrity. The librarian can track details such as how much of the budget has been spent, which controls have been tested and which have not, and which tests have passed and which have failed. The SOX project manager in charge of a large project should hire a part-time or temporary librarian before testing begins.

### **Step 10: Training Testers**

To save time, it's best to train the SOX team as a group before testing or re-documentation begins. The training should include a technical component covering new SOX guidance from the SEC, PCAOB and COSO. It should also include practical training in the SOX team's workpaper standards, persuasive evidence, testing methods and other topics covered in this article.

### **Parting Words**

Now is the time to begin planning for SOX compliance. By getting started in the second quarter, most calendar-year public companies can save time and money, while realizing more reliable results.

### **Bio for Bill Douglas**

Bill Douglas, CPA, CIA, CFE, is the founder of and president of Cost Advisors, a Portland firm focused on risk management, fraud and recovery. He is a frequent speaker and trainer on topics related to internal controls. Mr. Douglas is also the author of SOX Illustrated, a guide to understanding the Sarbanes-Oxley Act. Cost Advisors designed SarbOxPro<sup>®</sup>, a software application that helps companies meet Section 404 requirements. In his article, "SOX Compliance: 10 Steps to Savings," Mr. Douglas shares ten steps a company can take to save time and money on SOX compliance.

### **Sidebar**

AICPA members can download the PDF versions of COSO's 2006 and 2009 Guidance at [www.cpa2biz.com](http://www.cpa2biz.com) for only \$50 and \$35, respectively. The cost is slightly higher for non-members.