protiviti®
Risk & Business Consulting.
Internal Audit.

The Bulletin

Volume 5, Issue 10

Top 10 Lessons Learned From Implementing COSO 2013

Implementing the updated Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control – Integrated Framework (Framework) during 2014 has been an important endeavor for many public companies in their efforts to comply with Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). As background, the U.S. Securities and Exchange Commission (SEC) requires companies to use a "suitable framework" as a basis for evaluating the effectiveness of internal control over financial reporting (ICFR), as outlined in Section 404. The COSO Framework meets the SEC's criteria for suitability.

COSO has indicated that it no longer supports the original version of the Framework released in 1992 and considers it to be superseded by the updated version of the Framework, completed in 2013, for years ended after December 15, 2014. Accordingly, it is just a matter of time before all companies use the revised Framework for their annual evaluations of ICFR. Based on SEC filings to date, a strong majority of issuers have completed the transition from the 1992 version to the 2013 version. In this issue of *The Bulletin,* we share 10 lessons learned from these successful implementations from a variety of sources – working with our clients, information gathered from thousands of attendees at our webinar series, and our annual Sarbanes-Oxley Compliance Survey, available at www.protiviti.com/SOXsurvey.

It is presumed that everyone understands that a top-down, risk-based approach remains applicable to Section 404 compliance, and the transition to the 2013 updated Framework does not affect this. While we didn't list this as a lesson, we could have, because some companies either forgot or neglected to apply this approach when setting the scope and objectives for using the Framework. As a result, they went overboard with their controls documentation and testing. We can't stress enough that the 2013 COSO Framework did not change the essence of, and the need for, a top-down, risk-based approach in complying with SOX Section 404. We will reiterate this point a few times below.

10 Lessons Learned

1. Meet with your auditor early and often.
2. Establish an effective and relevant mapping approach.
3. Conduct a substantive fraud risk assessment.
4. Take a broader view of outsourced processes than just the service organization control (SOC) report.
5. Manage the level of depth when testing indirect controls.
6. Focus on understanding and documenting control precision.
7. Evaluate the adequacy of information produced by entity (IPE).
8. Expect an increase in deficiency evaluation efforts.
9. Adopt the updated 2013 Framework on time.
10. Ask yourself: Is limiting your focus on applying 2013 COSO to SOX compliance the answer?

Meet with your auditor early and often

Successful teams meet with their external auditors to present their approach, establish milestones and communicate progress and results on a periodic basis. This ongoing dialogue is important to ensure that the company and its independent auditor are fully aligned on the appropriate process for transitioning to the updated Framework, so that the evaluation of ICFR effectiveness can proceed with confidence. Open communication enables both parties to get on the same page and facilitates an understanding of the auditor's expectations, including recommended approach, documentation requirements and the extent of reliance on the work of internal audit and other parties.

In cases where the independent auditors elect to use the work of others, it is important to understand any specific requirements the auditors have relevant to that work, such as prescribed sample sizes and specific templates. We've noticed that some firms prefer that their audit clients use the firms' proprietary tools for mapping controls to the 17 principles, documenting review controls and performing walkthroughs.

Establish an effective and relevant mapping approach

After the updated 2013 Framework was released, there was quite a debate on how to transition from the original 1992 version. As a matter of expediency, most companies simply decided, in collaboration with their independent auditors, to map their controls to the 17 principles outlined in the 2013 Framework. With respect to mapping, there are several key points to consider:

- **Focus on the key controls –** The focus of the mapping should be on the existing key controls rather than the entire controls population. This makes sense if the key controls were determined in the prior year through a top-down, risk-based approach. Furthermore, a top-down, risk-based approach should drive the mapping exercise itself.
- **Understand the auditor's expectations –** In finalizing the mapping approach, the expectations of the external auditor should be considered to ensure the audit requirements are addressed without resorting to costly rework following the completion of the process.
- **Leverage the points of focus provided by the Framework –** A majority of companies have found that most of the points of focus are relevant to their circumstances. In addition, the external auditors inevitably ask to see how the points of focus were considered. While not mandatory, the points of focus are useful for those who choose not to start the process with a blank sheet of paper. The mapping exercise was manageable for most companies, requiring 80 to 300 hours to complete, depending on the size and complexity of the organization. It is interesting that companies using the points of focus as a form of guidance during the mapping process had a more efficient implementation approach than those organizations that didn't use them. The latter group of companies experienced more challenges.
- **Start with the existing controls documentation –** The principles should be mapped to the organization's existing controls documentation so management can evaluate whether the body of evidence supports a preliminary conclusion that the various principles are present and functioning. Ideally, the existing controls documentation can be expected to provide most, if not all, of the input to this mapping exercise, particularly if the company has previously documented its controls in a rigorous fashion using the 1992 version of the Framework. In completing the mapping exercise, provisions should be made for mapping a single control to multiple principles if it is relevant to those principles.
- **Manage the gaps –** If there are gaps for certain principles, the company will need to ascertain whether additional controls exist or require strengthening to support a conclusion that those principles are present and functioning. Once all gaps are addressed, management presumably is in a position to conclude the components are present and functioning. Interestingly, many companies found gaps in their entity-level controls when they did the mapping. In many cases, this was due to not taking credit for existing controls previously not included in scope for SOX purposes.
- **Consider the nature of the components when mapping the controls –** There is no one-size-fits-all solution for mapping controls to the 17 principles, as the structure, risks and operating style of each organization will have an impact on the appropriate process. Following are illustrative points regarding the application of the mapping process to each of the five components:
  - The Control Environment lends itself primarily to mapping directly to entity-level controls.
  - In the Risk Assessment component, the principle addressing objective setting for external financial reporting focuses on long-established financial reporting assertions and materiality considerations, and generally reflects entity-level activities. The other Risk Assessment-related principles could either be embedded in the Control Activities component documentation or evaluated separately from an entity-level perspective (as part of the Risk Assessment component documentation). For example, many organizations have integrated their fraud risk assessment into their Section 404 documentation rather than having a separate fraud risk assessment.
  - Most traditional controls supporting reliable financial reporting fall under the Control Activities component, which maps to three of the 17 principles. Some controls map to the two principles supporting the Monitoring component, while others map to the Information and Communication component-related principles that are either applied at the entity level or embedded in the various business cycles.
  - For Information and Communication-related controls, judgment is applied to determine where they are documented. For example, Principle 13 of the Information and Communication component addresses relevant, quality information to support the functioning of other components of internal control, particularly Control Activities and Monitoring. However management chooses to document these controls, care should be taken to ensure they are referenced in some way to the Information and Communication component.

The level of effort for transitioning the existing controls documentation to the principles-based 2013 Framework will depend on a number of factors, such as size and complexity of the company, the extent to which the issuer has kept the controls documentation current for changes in the business over time, and the expectations of the external auditor regarding the nature and extent of the documentation required.

Conduct a substantive fraud risk assessment

Principle 8 of the 2013 Framework states that "the organization considers the potential for fraud in assessing risks to the achievement of objectives." Thus, ongoing risk assessments as part of the top-down, risk-based approach need to consider explicitly the potential for fraud as it relates to ICFR. As a result, many companies raised the question as to whether separate documentation would be required to address Principle 8.

We now see fraud risks being called out more specifically to ensure the assessment is complete. In prior years, some companies did not flag anti-fraud controls; in effect, they integrated their evaluation of these controls with the evaluation of other controls within the organization's processes. Now, as part of the evaluation of the control activities related to identified fraud risks, the adequacy of anti-fraud controls is being specifically evaluated.

In practice, we've seen that the level of depth and rigor applied to these risks and controls has varied by company. It is likely that the Public Company Accounting Oversight Board (PCAOB) inspections of 2014 and 2015 year-end audits will drive the level of depth independent auditors will expect of their audit clients' fraud risk assessments.

Take a broader view of outsourced processes than just the service organization control (SOC) report

COSO references the concept of outsourced business processes in several places in the 2013 Framework. For example, COSO states that information obtained from outsourced service providers (those that manage business processes on behalf of the entity, and other external parties on which the entity depends in processing its information) is subject to the same internal control expectations as information processed internally. The point is clear: Management retains responsibility for controls over outsourced activities; therefore, these processes should be included in the scope of any evaluation of ICFR to the extent a top-down, risk-based approach determines they are relevant.

Why is it critical to take a broader view of outsourced provider relationships? These relationships present unique risks that often require selecting and developing additional controls to ensure completeness, accuracy and validity of information submitted to, and received from, the outsourced service provider.

Accordingly, risk assessments should consider these risks and the related control activities established to address the integrity of the data and information sent to and received from the outsourced service provider. Controls supporting the organization's ability to rely on information processed by external parties include vendor due diligence, inclusion of right-to-audit clauses in service agreements, exercise of right-to-audit clauses, and obtaining an independent assessment of the service provider's controls that sufficiently focuses on relevant control objectives (a Service Organization Controls report, typically referred to as a SOC 1 report).

An effective approach involves using a systematic methodology to evaluate SOC 1 reports and management controls around the outsourced providers. The organization needs to articulate how it oversees input and output controls in conjunction with the SOC 1 report. In evaluating the SOC 1 report, management may find there are some missing and/or deficient controls, and the service provider will need to provide additional information for clarification.

This evaluation should include ascertaining what account balances are touched by the work of the provider; the related internal control assertions (e.g., for financial reporting the assertions of completeness and accuracy, existence and valuation); how results are evaluated for reasonableness within established tolerances as dictated by the desired precision of the control activities in question; and whether the provider conforms to the organization's code of conduct.

The bottom line is this: If the organization extends its activities beyond its walls (and what company doesn't?), then it should also extend its control environment. The blurred lines of responsibility between the entity's internal control system and that of outsourced service providers creates a need for more rigorous controls over communication between the parties. We expect outsourced processes will receive increased focus in 2015 to further demonstrate management's understanding of the controls in place around its critical financial information.

Manage the level of depth when testing indirect controls

Testing of indirect controls (often referred to as entity-level controls) should be scaled commensurate with the extent of their relevance in reducing financial reporting risk to an acceptable level. Often, the relevance to risk mitigation is indirect, whereas control activities implemented at the source of risk are more direct in nature. The point is that the testing scope can get out of control quickly if the scope is not carefully rationalized through a top-down, risk-based approach focused sharply on the achievement of relevant control objectives.

We've noticed that successful organizations are more specific on the requirements for how an entity-level control is applied. For SOX compliance purposes, it is important to keep the focus of the indirect control environment on ICFR and not broadly expand the scope to cover non-ICFR-related issues. For example, for the indirect control emphasizing background checks, management can scope the application of this activity to the appropriate people charged with financial reporting responsibilities rather than all employees throughout the organization. Everyone agrees that the Control Environment component is important. However, the Control Activities component has a disproportionately higher impact on the assessment of ICFR than the indirect controls typically documented to define the Control Environment.

Focus on understanding and documenting control precision

Many organizations invested substantial time documenting increased precision around controls in line with this common theme raised by PCAOB inspection reports. The expectations of the external auditors around the level of detail captured in support of the conclusions drawn on control design effectiveness have increased to include evaluating the source of data inputs, such that an independent third party could reperform the evaluation and come to the same conclusion.

Therefore, management review controls received significant scrutiny, and many of these controls fell short of achieving a sufficient level of precision to substantiate an ability to detect material misstatements. The result is a shift to transactional-level controls in many cases, particularly when management does not have evidence that the review control has detected errors in the past. A review control's track record in detecting and correcting errors and omissions is vital to supporting an assertion that the control meets the prescribed level of precision.

Evaluate the adequacy of information produced by entity (IPE)

Information used in the execution of key controls, often referred to as IPE or electronic audit evidence (EAE), should be evaluated for completeness and accuracy. Historically, companies and their independent auditors have done varying levels of validation of this information. These efforts continue to focus on spreadsheets, due to their manual nature and susceptibility to error. Spreadsheets and other data sources that auditors rely upon, such as standardized or customized reports, have continued to be the source of financial restatements.

Adopting the 2013 COSO Framework has caused companies to evaluate IPE in more detail than in previous years, primarily because of the need to ascertain whether the Information and Communication component is present and functioning. More important, PCAOB inspection reports have also driven activity to validate system reports, queries and spreadsheets, and these efforts are blended into the overall COSO adoption activities. Inconsistencies remain among and within audit firms with regard to the level of rigor required to validate key information used in conjunction with the performance of control activities.

We do not believe the last word has been heard from the PCAOB on deficiencies in testing IPE. Therefore, we expect further emphasis in the next round of inspection reports on inherent reliance of key controls on IPE.

Expect an increase in deficiency evaluation efforts

Experience from the transition process indicates more analysis is required to evaluate identified deficiencies. COSO's terminology of "present and functioning" and "operating together" directly speaks to this. Organizations implementing the new Framework need to step back from the evaluation process and assess the results in a systematic manner. The PCAOB and SEC also have placed emphasis on deficiency evaluation for auditors and issuers, respectively, pointing to potentially correlated deficiencies that might result in broader implications when aggregated than the deficiencies individually might represent.

A common question is whether COSO changed the language around assessing ICFR deficiencies. This question arises because the 2013 Framework states that a deficiency is "a shortcoming in a component or components and relevant principle(s) that reduces the likelihood that the entity can achieve its objectives" and provides a structure for classifying the severity of deficiencies, with "major deficiency" defined as "an internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives."

COSO stressed that its intent was to release a framework that could cross international borders. In doing so, it did not intend in any way to alter the "material weakness" and "significant deficiency" lexicon used in the United States around financial reporting controls.

One last point: "Operating together" recognizes that components are interdependent with a multitude of interrelationships and linkages, particularly in terms of how principles interact within and across components. From a practical standpoint, the 2013 Framework states that management can demonstrate that the components operate together when they are present and functioning, and internal control deficiencies aggregated across components do not result in the determination that one or more major deficiencies exist.

Adopt the updated 2013 Framework "on time"

A strong majority of organizations have adopted the revised Framework "on time," in line with COSO's cessation of its support of the 1992 Framework, with a handful of early adopters leading the way. Of just over 3,500 annual reports by companies with fiscal year-ends after December 15, 2014 and filed through April 2, 2015,[1] 77 percent had transitioned to COSO 2013. Of the remaining 23 percent:

- Seventy-eight percent (or 18 percent of the total filings) reported their continued use of the 1992 Framework.
- Twenty-two percent (or 5 percent of the total filings) did not identify the version of the Framework they used.

It is possible that some, if not many, of these latter filers may have transitioned to the 2013 Framework and did not disclose they had done so because the transition period had run its course and, therefore, the parenthetical disclosure in the internal control report was considered by these filers to be unnecessary. If any of these filers continued to use the 1992

[1] As reported by Audit Analytics® in its internal controls management report and audit report database, available by subscription (www.auditanalytics.com).

Framework, their lack of disclosure in their internal control report could pose a concern for the SEC staff.

Bottom line is, regardless of how the data is cut, we can report that a strong majority of filers have transitioned to the 2013 Framework. As we noted earlier, for most of these companies the level of effort in completing the transition was manageable.

The implication of the ratio of "on time" transitions to companies that remain to complete their transitions is clear: They need to get on with it. We are confident that, given the strong majority of companies that have transitioned successfully and their experience in completing the transition process, the SEC staff will not provide a "free pass" for year-ends after December 15, 2015, except perhaps in the most extreme circumstances.

Ask yourself: Is limiting your focus on applying 2013 COSO to SOX compliance the answer?

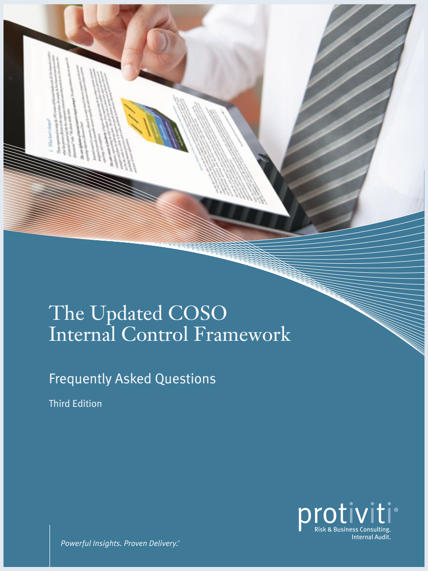
Most organizations have limited their focus on using COSO 2013 to SOX. Due to the increased work required to map to the updated Framework and address management review control precision, IPE and other concerns raised by the PCAOB inspection reports, many organizations have not applied the Framework more broadly.

Interestingly, some were confused by the Risk Assessment component's objectives around operations and compliance, and mistakenly thought they were in scope for SOX – as if they thought COSO's Framework was designed exclusively for SOX compliance. This is not the case.

We believe there are benefits to using COSO for other objectives (e.g., operations, compliance, and internal and other external reporting). However, these efforts should be segregated from SOX compliance. Progressive organizations are applying COSO to other objectives, such as sustainability reporting, regulatory compliance and controls over federal grants, to name a few.

Summary

The first year of transition to the 2013 Framework since the cessation of support by COSO for the 1992 version continues to roll forward. Much has been learned from the experience of the strong majority of filers that have transitioned successfully. This issue of *The Bulletin* has summarized some of the key lessons learned. While many of these lessons are not necessarily new, they are nonetheless just as important in the transition process as they have been over the years in implementing the SOX Section 404 compliance process. We hope they will be of value to organizations that have yet to transition.


The Updated COSO
Internal Control Framework
Frequently Asked Questions
Third Edition
protiviti
Risk & Business Consulting.
Internal Audit.
Powerful Insights. Proven Delivery.®

COSO Framework Adoption – Strong So Far

A strong majority of organizations have adopted the revised framework on time, with a handful of early adopters leading the way. Of just over 3,500 companies with fiscal year-ends after December 15, 2014 that filed annual reports through April 2, 2015, only 18 percent report they have not transitioned to COSO 2013.

COSO has indicated that it no longer supports the original version of the Framework released in 1992 and considers it to be superseded by the 2013 Updated COSO Framework for fiscal years ended after December 15, 2014. Accordingly, it is just a matter of time before all companies use the revised Framework for their annual evaluations of ICFR.

Protiviti's Third Edition of *The Updated COSO Internal Control Framework: Frequently Asked Questions* (available at www.protiviti.com/en-US/Pages/The-Updated-COSO-Internal-Control-Framework-FAQ.aspx) addresses various questions regarding the 2013 Framework from COSO, including the reasons why it was updated, what has changed, the process for transitioning to its use, and the steps companies should be taking now.

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.