

# Internal Auditors, Are You Ready for the Updated COSO Framework?

[Jose Tabuena](#)

May 13 2014



**Jose  
Tabuena**  
Columnist

Even if the updated COSO framework is already *de rigueur* at your organization, internal auditors need to be prepared to address inquiries by management and shareholders regarding transition to the new framework.

With the proxy season approaching, one of the areas shareholders are planning to address at annual meetings is whether companies are in compliance with the 2013 framework for internal controls. If not, why, and what changes will be needed to comply? And what are the timeframes and costs to do so? In preparation, boards are asking these same questions.

The Committee of Sponsoring Organizations' updated *Internal Control – Integrated Framework* was published last year to refine the original 1992 framework. COSO has stated that the 1992 framework will be superseded as of Dec. 15, 2014. Thus companies, particularly U.S. public issuers who relied on the original framework to achieve Sarbanes-Oxley Act compliance, will be expected to transition to the new framework in time for 2014 year-end reporting. Moving forward, it will not be practicable for any issuer to take the position that the 1992 framework qualifies under SEC criteria as a “suitable framework” for purposes of complying with Section 404 of Sarbanes-Oxley.

Your management team might still find itself unprepared for the changes wrought by COSO's framework update and struggling to fully understand the new requirements or significant clarifications. Internal auditors should take the initiative in communications with management to ease the transition. We know that ultimately controls are management's responsibility, but management should and does rely on internal audit for advice about the standards for implementing effective internal controls.

## Why Even Update?

The original version released in 1992 had gained broad acceptance and has been widely used as the predominant framework for reporting on internal control over financial reporting in accordance with Sarbanes-Oxley as well as for other similar regulatory requirements outside the United States. Although COSO did not consider the framework to be “broken,” their decision to update it was driven by the extent of change in the business environment over the past two decades.

Some of the noted trends and events that drove the decision to update the framework include:

- More expectations for governance oversight especially following large-scale internal control and compliance breakdowns
- Risk-based approaches receiving more attention
- Globalization of markets and operations
- Third-party risks emerging including from the use of outsourcing and strategic suppliers
- Enhanced technology creating new and different risks
- And the continuing and increasing demands and complexities in laws, regulations, and standards

These trends along with highly publicized governance failures have led to the reinforcement of themes that are becoming recognized as essential to creating a strong internal control environment. The framework enhancements apply lessons derived from these core topics which include the importance of corporate culture, addressing the insidious impact of conflicts of interests, siloed risk management, ineffective board oversight, unbalanced compensation structures, management override, all of which have a strong potential to enable dysfunctional and rogue behavior.

### **New Versus Old**

While the 2013 framework retains much of the original and builds on what has proven useful, its fundamental difference is a widened scope and greater applicability of the updated framework.

The core definition of internal control, for example, remains in conjunction with its five components. Under the new framework, organizations continue to establish relevant objectives relating to operations, financial reporting, and compliance. As before, these objectives can be set for the entity as a whole, or targeted to specific divisions, functions, or operating units. These discrete areas cumulate into that well-known three-dimensional cube. Management can find comfort that the criteria to assess the effectiveness of an internal control system remain largely unchanged. The new framework further continues to emphasize the importance of management's judgment in evaluating the effectiveness of a system of internal control.

### **While the 2013 framework retains much of the original and builds on what has proven useful, its fundamental difference is a widened scope and greater applicability of the updated framework.**

The most significant change is the explicit articulation of 17 principles that provide the foundation associated with the five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities. All the principles apply to each category of the three objectives. COSO decided to make these “principles” explicit to enhance management's understanding as to what comprises effective internal control. Then supporting each principle are points of focus (77 in all) that are intended to provide guidance to management in designing and implementing internal controls.

It would be a good practice for internal audit to consider and discuss the principles with senior management and the board or audit committee particularly those that address risk to the more significant objectives of the organization. The new framework incorporates an enhanced

discussion of governance concepts, and considers the increased relevance of technology, anti-fraud measures, and non-financial reporting objectives. The significance of governance and how it relates to compliance activities to support effective internal control is also more pronounced in the new framework.

## **The Transition**

Most audit professionals recommend that to start the transition companies should map their controls to the 17 COSO principles—albeit focusing first on areas where there is a reasonable possibility of a material mis-statement. Word is that early adopters of the updated framework indicate that their existing internal controls generally map quite well to the revised principles in the framework. Some companies have reported that, following the mapping, their controls appear sufficient with the components operating together although some of them were not scoped into the internal assessment and audit.

By and large it doesn't appear that new activities are required. It does mean identifying and streamlining activities already undertaken that support the COSO principles, and then documenting them and bringing them into scope. Some have observed that more effort is needed to align existing controls rather than to create new ones.

One area internal audit should consider providing more clarification for management is the effect of new COSO on the term *material weakness*. Over the years, companies have become familiar with the terms “deficiency” and “significant deficiency,” as they complied with Sarbanes-Oxley Act requirements to assess the effectiveness of internal controls. Now COSO has added a “major deficiency” to the internal control lexicon, as companies consider whether those deficiencies and significant deficiencies can add up to a material weakness. Because this is new terminology, it is requiring training and education to fully understand it and how the terms interplay with Sarbanes-Oxley or other rules that have their own definitions.

## **Overlaps With Compliance Effectiveness Remain**

COSO is advocating the use of the new framework beyond the worlds of internal control and risk management. COSO says its frameworks can be used to improve overall organizational performance and corporate governance and support companies on a path to better achievement of business goals over the long term. It has also published *Enterprise Risk Management – Integrated Framework* and explained the links between the two frameworks and how they can be more broadly applied.

A corporate compliance program itself should be viewed as a broad control that supports the principle of organizations demonstrating a commitment to integrity and ethical values—and also serves as an anti-fraud program control.

The evaluation of the control environment is one that should be leveraged by internal audit to apply to compliance program effectiveness under the U.S. Federal Sentencing Guidelines criteria as well to fraud control standards from the audit profession. To demonstrate that a COSO principle is present and functioning, the organization must understand the intent of the principle

and how it is being applied. Auditors can refer to the points of focus in the new framework to enhance their understanding.

Keep in mind that that the points of focus under the first principle, “The organization demonstrates a commitment to integrity and ethical values,” is redundant with the promotion of ethical conduct under the Federal Sentencing Guidelines. The new COSO framework provides four points of focus:

- Sets the “tone at the top”
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner

A team of internal or external auditors would be remiss in not partnering closely with compliance professionals when evaluating whether this principle is present and functioning. The principle and associated points of focus are encompassed under the elements of a compliance and ethics program. For example, if a company has established a code of conduct *how* do you know if it is truly effective and it is understood and followed by employees; and *how* do you determine if the appropriate tone has been set at the top and the middle? These are areas where the compliance function has developed deep expertise over the past two decades.