The NEW COSO Internal Control – Integrated Framework

And Why it Deserves Attention from Public and Privately Held Companies

While internal controls can never be failsafe or provide absolute assurance, they are still the best defense and protective measure against fraud that an organization can put into place. And although private organizations may not have the same level of requirements as public registrants related to internal controls, they should still pay attention to the Committee of Sponsoring Organizations (COSO) of the Treadway Commission's new framework released in May.

The original COSO Internal Control – Integrated Framework (1992) has been the leading framework for designing, implementing and conducting internal control and assessing the effectiveness of internal control. The COSO framework has been used broadly with both private and public organizations and it was accepted by the SEC as a framework for attesting to internal control over financial reporting as required by the Sarbanes-Oxley Act of 2002 (SOX).

But in the last twenty years, much has changed – business and operating environments have become increasingly complex, technologically driven and global. Additionally, stakeholders are more engaged than ever, demanding transparency and accountability.

In May, COSO released their new integrated framework to appropriately reflect the changes that have occurred in the last two decades. And although the new framework is an improvement, the 1992 version will remain appropriate and relevant for a transition period that will end December 15, 2014.

WHY IS IT IMPORTANT FOR PRIVATE COMPANIES?

Internal controls not only reduce the risk of loss, but help ensure that information is complete and accurate, financial statements are reliable and that an entity complies with laws and regulations. Public registrants have more stringent requirements related to internal controls and essentially must pay attention to the COSO framework.

But fraud and risk of loss is not exclusive to large, public companies.

According to the ACFE's Report to the Nations on Occupational Fraud and Abuse (2012 Global Fraud Study), "…the typical organization loses 5 percent of its revenue to fraud each year." and "Occupational fraud is a significant threat to small business." In fact, they report the smallest organizations suffered the largest median losses.

With fewer resources, the losses experienced by small businesses tend to have a greater impact than they would in larger organizations. And smaller organizations typically employ fewer and less effective anti-fraud controls than their larger counterparts, which increases their vulnerability.

Keeping up with this ever-changing environment is one of the best ways to protect an organization. As such, internal controls should be a process of continuous improvement by organizations large and small. Implementing and layering in the new framework is an excellent opportunity to improve a functioning system or fix a broken or insufficient system of internal controls.

Further, while COSO is not a standard setter and does not have the power to require an organization to switch to the new framework, organizations might have some difficulty explaining to their stakeholders why they are not using the new framework.

WHY THE FRAMEWORK HAD TO CHANGE

Competitive pressures, advances in technology and regulatory scrutiny have contributed to increasing expectations for providing relevant information immediately. Additionally, investors, owners, regulators and other users continue to demand more and quality reporting.

The new framework reflects the many changes in the business and operating environments of the past several decades, including:

- Expectations for governance oversight
- Globalization of markets and operations
- Changes and greater complexities of business
- Demands and complexities in laws, rules, regulations and standards
- Expectations for competencies and accountabilities
- Use of, and reliance on, evolving technologies
- Expectations related to preventing and detecting fraud

WHAT CHANGED … AND WHAT DIDN'T

Those experienced at using the 1992 framework will find a lot of familiarities in the new framework, as it builds on what has proven effective in the original.

What is not changing…	What is Changing…
Core definition of internal controls	Operations and reporting objectives expanded
Three categories or objectives and five components of internal controls	Changes in business and operating environments considered
Each of the five components of internal controls are required for effective control	Fundamental concepts underlying five components articulated as principals
Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness	Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added

The new framework sets out seventeen principles representing the fundamental concepts associated with each of the five components. The framework views the seventeen principles as suitable to all entities (except in rare circumstances) and, as such, a principle that is not present or functioning is deemed to be a "major deficiency" in internal controls. The framework also indicates that a major deficiency cannot be mitigated by other principles or controls. While the definition of deficiency in internal control varies from the COSO framework to audit standards, many professionals are of the opinion that a missing principle would likely equate to a material weakness in internal controls under audit standards and therefore would likely be a reportable condition.

The new framework also describes points of focus that are important characteristics of principles. Not all points of focus will be suitable or relevant for each organization and organizations may identify and consider other points of focus.

WHAT CHANGED … AND WHAT DIDN'T (con't.)

The points of focus are intended to assist management in designing, implementing and conducting internal control and in assessing whether the relevant principles are, in fact, present and functioning.

The following is a table illustrating each of the seventeen principles and how they related to the five components:

Components	Principles	No. of Points of Focus
Control Environment	Demonstrates commitment to integrity and ethical values Exercises oversight responsibility Establishes structure, authority and responsibility Demonstrates commitment to competence Enforces accountability	4 4 3 4 5
Risk Assessment	Specifies suitable objectives Identifies and analyzes risk Assess fraud risk Identifies and analyzes significant change	5 5 4 3
Control Activities	Selects and develops control activities Selects and develops general controls over technology Deploys through policies and procedures	6 4 6
Information/ Communications	Uses relevant information Communicates internally Communicates externally	5 4 5
Monitoring Activities	Conducts ongoing and/or separate evaluations Evaluates and communicates deficiencies	7 3

The new framework includes companion documents with approaches, examples and illustrative tools. The ideas and examples help organizations apply the framework to their specific situations. The illustrative tools contain templates that organizations can use to evaluate and document the effectiveness of internal control.

SO NOW WHAT?

The process of evaluating the new framework and implementing the new components can be overwhelming, especially for smaller organizations.

And, even though public registrants may be better versed and have more resources to address the new framework, the level of responsibility and compliance related to implementing the new framework isn't going to be as simple as copy, paste and assemble. It will be critically important that public registrants identify and remediate gaps and appropriately pressure test changes in preparation for transition. Due to independence rules, public registrants will likely need to consult with second source providers as they proceed through transition to ensure preparedness for external audit.

SO NOW WHAT? (con't.)

To assist organizations in their transition to the new framework, COSO released an article "One Approach to an Effective Transition" in June 2013. This article lays out a "Five-Step Transition" plan for organizations to consider.

The Five-Step Transition Plan
Step 1: Develop awareness, expertise and alignment
Step 2: Conduct preliminary impact assessment
Step 3: Facilitate broad awareness, training and comprehensive assessment
Step 4: Develop and execute COSO transition plan for SOX compliance
Step 5: Drive continuous improvement

CALL TO ACTION

Those who currently use the COSO's 1992 Framework should complete their transition to the new 2013 version no later than December 15, 2014, at which time the original Framework will be superseded.

The framework is available for purchase at www.coso.org, where an executive summary and the article on effective transitions are available free of charge.

****

For more information or assistance on implementation, contact:

Danielle J. Kimmell, CPA
Partner
Assurance Services
330.255.2459
dkimmell@bobermarkey.com