KPMG
cutting through complexity

Defining Issues®
May 2013, No. 13-26

COSO Releases Internal Control – Integrated Framework (2013)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recently released its updated Internal Control – Integrated Framework (2013 Framework).[1] COSO also issued these companion documents:

- Executive Summary;
- Internal Control – Integrated Framework: Illustrative Tools for Assessing Effectiveness of a System of Internal Control (Illustrative Tools), which provides templates to assist users in documenting their assessment of principles, components, the overall system of internal control, and scenarios of how the templates could be used; and
- Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples (the Compendium), which features examples of internal control over financial reporting and illustrates how users might apply the principles of the 2013 Framework to external financial reporting objectives.

The changes made to update the 1992 Framework are evolutionary, not revolutionary. The 2013 Framework takes into account changes in the business environment and operations over the last 20 years. The 2013 Framework retains the definition of internal control and the COSO cube, including the five components of internal control: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.

Contents

[1] Internal Control – Integrated Framework (2013) was released by COSO on May 14, 2013. The 140-page Framework includes these appendices: A: Glossary; B: Roles and Responsibilities; C: Considerations for Smaller Entities; D: Methodology for Revising the Framework; E: Public Comment Letters; F: Summary of Changes to the COSO Internal Control – Integrated Framework (1992); and G: Comparison with COSO Enterprise Risk Management – Integrated Framework. For more information, see the press release and executive summary at www.coso.org.

The most significant change made in the 2013 Framework is the codification of the 17 principles that support the five components. The 17 principles were fundamental concepts implicit in the 1992 Framework. For effective internal controls, the 2013 Framework requires that (1) each of the five components and the 17 relevant principles be *present* and *functioning*; and (2) the five components must operate together in an integrated manner. Present means that the components and relevant principles exist in the design and implementation of the system of internal control, and functioning means that the components and relevant principles continue to exist in the conduct of the system of internal control. The 2013 Framework also provides example characteristics for each of the 17 principles, called Points of Focus, to assist management in determining whether a principle is present and functioning. The judgment required by management, the board of directors, and other personnel to design, implement, and conduct the internal controls and assess their effectiveness has not changed. Appendix F of the 2013 Framework summarizes the significant changes and emphasis from the 1992 Framework.

SEC registrants may use the 1992 Framework or the 2013 Framework to evaluate the effectiveness of their internal control over financial reporting during the transition period ending December 15, 2014.[2] Thereafter, the 1992 Framework is considered superseded by the COSO Board. Registrants should describe the applicable Framework used during the transition period by identifying the year of the Framework in the title.

In adopting the 2013 Framework, COSO followed due-process procedures during the five phases of the project described in Appendix D, including broad distribution of the Framework for public comment. The Framework was exposed for public comment twice – in September 2012 and December 2011.

Definition of Internal Control and Objectives

Internal control is defined in the 2013 Framework as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

The COSO Framework is designed to be used by organizations to assess the effectiveness of the system of internal control to achieve objectives as determined by management. The 2013 Framework lists three categories of objectives, similar to the 1992 Framework:

- ***Operations Objectives –*** related to the effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss. In the 1992 Framework, the operations objective was limited to "effective and efficient use of the entity's resources."

[2] This evaluation is required by SEC Regulations 13a-15 and 15d-15.

- ***Reporting Objectives –*** related to internal and external financial and nonfinancial reporting to stakeholders, which would encompass reliability, timeliness, transparency, or other terms as established by regulators, standard setters, or the entity's policies. In the 1992 Framework, the reporting objective was called the financial reporting objective and it was described as "relating to the preparation of reliable financial statements."
- ***Compliance Objectives –*** related to adhering to laws and regulations that the entity must follow. In the 1992 Framework, the compliance objective was described as "relating to the entity's compliance with applicable laws and regulations." The 2013 Framework considers the increased demands and complexities in laws, regulations, and accounting standards that have occurred since 1992.

The COSO Framework is most commonly used by management of SEC registrants to assess the effectiveness of internal controls over financial reporting on an annual basis as required by the SEC. While the 2013 Framework expands the financial reporting objectives related to internal financial and nonfinancial reporting, registrants using either the 1992 or 2013 Framework to evaluate the effectiveness of internal controls over external financial reporting based on SEC Regulation 13a-15 still must meet the SEC's objectives for effective internal control over financial reporting, which have not changed.

Specifically, Regulation 13a-15(f) defines the term internal control over financial reporting as "a process designed by, or under the supervision of, the issuer's principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (GAAP)." The SEC definition also requires that registrants' processes include policies and procedures that:

(1) Provide for the maintenance of records that in reasonable detail accurately and fairly reflect transactions and dispositions of the assets of the issuer;

(2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and

(3) Provide reasonable assurance about prevention or timely detection of unauthorized acquisition, use, or disposition of the issuer's assets that could have a material effect on the financial statements.

The objective of effective internal control over financial reporting by SEC registrants is based on this definition of internal control.

Components

The five components of internal control are the same in both the 1992 and 2013 Frameworks; however, the 1992 definitions have been expanded in the 2013 Framework to address the following broad-based changes:

- Globalization of markets and operations – changes in operating models and organizational structures and risk factors as a result of globalization of markets and operations;
- Governance concepts – enhanced governance concepts imposed by regulators and more sophisticated global organizations;
- Different business models and organizational structures – expanded to include third-party service providers and partnering arrangements;
- Laws and regulations – expanded demands and complexities in laws, regulations, and standards to promote greater stakeholder protection and confidence in external reporting;
- Competence and accountability of personnel – demands for greater competence and accountabilities as organizations become more complex and operate under more advanced processes and technologies;
- Information systems – increased relevance and sophistication of technology across the entity and its processes; and
- Fraud risk – enhanced consideration of the potential for fraud in risk assessment and the organization's response to mitigate that risk.

Control Environment. "The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct."

The seven factors in the 1992 Framework relating to an effective control environment are integrity and ethical values; commitment to competence; board of directors or audit committee; management's philosophy and operating style; organizational structure; assignment of authority and responsibility; and human resource policies are captured in the five principles relating to Control Environment in the 2013 Framework.

The five principles relating to Control Environment are:

(1) The organization demonstrates a commitment to integrity and ethical values.

(2) The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

(3) Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

(4) The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

(5) The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

The 2013 Framework links the various components of internal control and demonstrates that the control environment is the foundation for a sound system of internal control.

Risk Assessment. "Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives."

The 1992 Framework focused on three areas: management's process for objective setting at an entity-wide and activity level; risk analysis; and managing change. The 2013 Framework recognizes that many organizations are taking a risk-based approach to internal control and that Risk Assessment includes processes for risk identification, risk analysis, and risk response; that risk tolerances and an acceptable level of variation in performance should be considered in the assessment of acceptable risk levels; and the discussion of risk severity includes velocity and persistence in addition to impact and likelihood. Most significantly, the Risk Assessment component now includes a separate principle to address the risk of fraud in the organization (Principle 8).

The 2013 Framework includes more extensive discussion about the types of fraud (fraudulent financial reporting, misappropriation of assets, and illegal acts) and management override of controls and the organization's response to fraud risk. The 2013 Framework states, "A system of internal control over financial reporting is designed and implemented to prevent or detect, in a timely manner, a material omission from or a misstatement of the financial statements due to error or fraud." Assessment of this principle may require additional attention by organizations that did not focus their assessment of fraud risk at the specific financial statement account, transaction, or assertion level.

The four principles relating to Risk Assessment are:

(6) The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

(7) The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

(8) The organization considers the potential for fraud in assessing risks to the achievement of objectives.

(9) The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities. "Control activities are the actions established by the policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities."

The fundamental concepts in the 1992 Framework related to Control Activities have not changed in the three principles listed in the 2013 Framework. However, the most significant changes to this component result from changes in technology over the last 20 years and include:

- An updated discussion on general information technology controls (GITCs) from 1992 to today's technology; and
- An expanded discussion of the relationship between automated controls and GITCs and how they link to the business processes. In connection with the organization's evaluation of effective internal control over financial reporting, we believe that this change in emphasis provides an efficient approach for management to focus on the effectiveness of automated controls at the financial statement assertion level, and linking those application controls to relevant GITCs. It is not necessary to identify and test all GITCs but rather only those that are relevant to risks related to financial reporting objectives.

As a result of Sarbanes-Oxley reform, SEC registrants have a deeper understanding of how control activities are effectively designed and implemented. However, we believe that many registrants have focused their attention on the effectiveness of the Control Activities component in the assessment of internal control over financial reporting at the expense of the other four components. The 2013 Framework's requirement for all relevant principles to be present and functioning and the requirement for all components to function in an integrated manner will encourage greater attention and emphasis on the effectiveness of internal control over financial reporting across the 17 principles and five components, beyond Control Activities.

The three principles relating to Control Activities are:

(10) The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

(11) The organization selects and develops general control activities over technology to support the achievement of objectives.

(12) The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Information and Communication. "Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day internal control activities. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives."

The importance of having the right information communicated to managers at the right time has become a key to successful business operations and effective internal control as organizations have become more complex in their structure and global operations and more dependent on technology. Changes in the Information and Communication component include:

- An expanded discussion about the verification of the source of information and its retention when information is used to support reporting objectives to external parties;
- Additional discussion about the impact of regulatory requirements on the reliability and protection of information;
- An examination of the impact of technology and other communication mechanisms on the speed, means, and quality of the flow of information; and
- Additional consideration of how the organization interacts with third-party service providers outside of its legal and operational boundaries.

The three principles relating to Information and Communication are:

(13) The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

(14) The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

(15) The organization communicates with external parties about matters affecting the functioning of internal control.

Monitoring Activities. "Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board."

COSO always intended that monitoring activities would address how all of the components of internal control are applied and whether the overall system of internal control operates effectively. The 2013 Framework distinguishes between a management review control as a control activity and a monitoring activity. A management review control that is a control activity responds to a specified risk and is designed to detect and correct errors. However, a

management review control that is a monitoring activity would ask why the errors exist, and then assign the responsibility of fixing the process to the appropriate personnel. A monitoring activity assesses whether the controls in each of the five components are operating as intended.

Ongoing evaluations are built into the routine operations and are performed on a real-time basis. A separate evaluation is conducted periodically by objective management personnel, internal audit, and external parties. The scope and frequency of separate evaluations is a matter of management judgment.

The two principles relating to Monitoring Activities are:

(16) The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

(17) The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Limitations of Internal Control

The 2013 Framework acknowledges that there are limitations related to a system of internal control. For example, certain events or conditions are beyond an organization's control, and no system of internal control will always do what it was designed to do. Controls are performed by people and are subject to human error, uncertainties inherent in judgment, management override, and their circumvention due to collusion. In designing, implementing, and conducting an effective system of internal control, management recognizes the system's inherent limitations and addresses ways to minimize these risks. However, an effectively designed system will not eliminate these risks. An effective system of internal control (and an effective system of internal control over financial reporting) provides reasonable assurance, not absolute assurance, that the organization will achieve its defined operating, reporting, and compliance objectives.

Major Deficiency and Material Weakness

The 2013 Framework requires for an effective system of internal control that each of the five components and the 17 relevant principles be present and functioning and that the five components operate together in an integrated manner. Present means that the components and relevant principles exist in the design and implementation of the system of internal control, and functioning means that the components and relevant principles continue to exist in the conduct of the system of internal control. A *major deficiency* is defined as an internal control deficiency or combination of deficiencies that severely reduces the likelihood that the entity can achieve its objectives. A major deficiency exists when management determines that a component and one or more relevant principles are not present and functioning or that components are not operating together.

In connection with management's evaluation of the effectiveness of internal control over financial reporting under Regulation S-K, Item 3-09, the SEC and auditing standards established *material weakness*, significant deficiency, and control deficiency where a material weakness is defined as "a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the registrant's annual or interim financial statements will not be prevented or detected on a timely basis." The 2013 Framework acknowledges that the criteria for defining and classifying the severity of internal control deficiencies established by regulators and standard-setting bodies, such as the SEC and the PCAOB, should be followed when reporting under those regulations or standards rather than relying on the 2013 Framework's classifications and definitions of internal control deficiencies.

Any internal control deficiency that results in a system of internal control not being effective for regulatory purposes also would preclude the organization from concluding that its internal controls were effective under the 2013 Framework.

A major deficiency in one component cannot be mitigated to an acceptable level by the presence and functioning of another component; likewise, a major deficiency in one principle cannot be mitigated to an acceptable level by the presence and functioning of other principles. We questioned how this statement would apply to an SEC registrant's evaluation of the severity of an identified control deficiency in connection with its annual reporting on the effectiveness of internal control over financial reporting. We believe that the registrant will first consider whether any other controls mitigate the risk of misstatement to an acceptable level as it has always done. In searching for mitigating controls, registrants are not limited to controls related solely to that principle or that component. Some controls, by their design, may be effective and affect more than one principle and component. Some have questioned whether this is contrary to the COSO statement that a major deficiency in a component or a principle cannot be mitigated by the presence and functioning of another component or principle. We believe that the COSO statement assumes that the organization will look for mitigating controls and, if none are found, only then could it conclude that a major deficiency (i.e., a material weakness) in one component or principle exists and is not mitigated.

Documentation

The 2013 Framework points out that effective documentation of the organization's system of internal control is necessary to provide evidence of its effectiveness, to enable proper monitoring, and to support reporting to stakeholders, regulators, and the entity's auditors on the effectiveness of internal control over financial reporting. Effective documentation of internal control also is useful for assigning responsibility and accountability to employees; training new and experienced employees who implement and

monitor the controls; promoting consistency across the organization; and retaining organizational knowledge.

While the level of documentation under the 2013 Framework will vary based on the size and complexity of the organization, the explicit nature of its principles will require the organization to address whether the internal controls related to the relevant 17 principles and five components are present and functioning at transition and going forward. The explicit nature of the principles also may cause the organization to reconsider the nature and effectiveness of previously identified internal controls over financial reporting, and to revise the documentation of those controls.

Transition – Timeline and Effort

Organizations will need to develop a plan to transition their assessments of the effectiveness of internal control over financial reporting from the 1992 Framework to the 2013 Framework. The explicit nature of the principles in the 2013 Framework will require the organization to address whether internal controls related to the relevant 17 principles are present and functioning and to refine the documentation of their assessment. This assessment during the transition period may cause the organization to reconsider the nature and effectiveness of previously identified internal controls over financial reporting and to identify new controls that are more effective or efficient. There is an opportunity to identify operational improvements in the system of internal control during the transition period.

SEC registrants also should be mindful that the transition assessment may identify control deficiencies or gaps where there are no controls that sufficiently address the risk related to an explicit modification made under the updated 2013 Framework. Management will need to consider the implications of any control deficiencies identified during the transition period and consider whether they also could be control deficiencies under the implicit fundamental concepts of the COSO 1992 Framework. Early assessment of the COSO 2013 Framework is encouraged for those reasons.

The COSO Board announced that it will continue to make the original 1992 Framework available until December 15, 2014. After that date, COSO will consider the 1992 Framework superseded. The Board stated that the key concepts and principles embedded in the 1992 Framework are fundamentally sound and broadly accepted in the marketplace, and continued use of the 1992 Framework during the transition period will be appropriate.

Absent guidance from regulators, we believe that SEC registrants using a COSO Framework to report on the effectiveness of their internal control over financial reporting as of the end of fiscal years falling in the transition period, May 14, 2013, to December 15, 2014, will have a choice to apply the 1992 Framework or the 2013 Framework but must specify which one they used.[3] Registrants with a calendar year-end may choose to continue to evaluate the effectiveness of internal control over financial reporting using the 1992 Framework for the fiscal 2013 assessment as of December 31, 2013; it will be required to use the 2013 Framework to evaluate the effectiveness of internal control over financial reporting for the fiscal 2014 assessment because the 1992 Framework will be superseded at the end of the transition period, December 15, 2014.

Under Regulation S-K, Item 308(c), registrants are required to disclose changes in internal control over financial reporting identified in connection with the annual evaluation that have materially affected, or are reasonably likely to materially affect, their internal control over financial reporting occurring during the interim reporting period. During the transition period we may see an increase in such disclosures as registrants adopt changes in internal control over financial reporting that are responsive to the new Framework.

We believe that the release of the 2013 Framework will result in management, auditors, and regulators taking a fresh look at the assessment of the effectiveness of internal control over financial reporting. If the organization's documentation of internal control has kept pace with increased globalization, changes in laws, regulations, technology, and other significant changes, then its transition to the 2013 Framework may be a simple mapping exercise of matching its internal control over financial reporting as documented under the 1992 Framework to the 17 codified principles. However, we expect that the transition to the 2013 Framework will require more extensive effort, analysis, and documentation.

KPMG Audit and Advisory professionals are available to respond to your questions and to assist you with your organization's adoption of the COSO 2013 Framework.

[3] SEC Regulation S-K, Item 3-09.

Contact us:
This is a publication of KPMG's
Department of Professional Practice
212-909-5600

Contributing authors:
Joseph Duggan
George Herrmann
Alan Lewis
Christian Peo
Sharon Todd
Marc Wittenberg
Harold Zeidman

Earlier editions are available at:
http://www.kpmginstitutes.com/financial-reporting-network