COSO's 2013 Internal Control Framework in Depth:

Implementing the Enhanced Guidance for Internal Control over External Financial Reporting

experience BKD LLP
CPAs & Advisors

Table of Contents

Executive Summary

COSO's Internal Control Framework has been updated and enhanced. Since its release in 1992, the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control – Integrated Framework* (the framework) has been widely accepted and adopted around the world. The updated framework, issued on May 14, 2013, maintains the fundamental elements of the original: five components of an internal control system—control environment, risk assessment, control activities, information and communication—and monitoring activities supporting three categories of objectives: effectiveness and efficiency of operations, reliability of reporting and compliance with applicable laws and regulations, structured through management's judgment.

The five components are evaluated through principles and recommended points of focus. A significant enhancement, however, is the expansion of the reporting objective to include nonfinancial and internal reporting objectives. The mandatory principles have been updated to reflect today's business environment—an environment of increased governance, regulatory and compliance demands and increased use of technology and complex business models. The original framework still may be used through December 15, 2014; beyond that date, COSO will consider the original framework obsolete.

Background

Accepted by the Securities and Exchange Commission (SEC), the framework has been widely adopted since its original issuance in 1992 to support external financial reporting internal control requirements. Section 404 of the Sarbanes-Oxley Act (SOX) requires public company management and its external auditors to attest to the design and operating effectiveness of a company's internal control over external financial reporting (ICEFR).

External financial reporting also is required by private, not-for-profit and governmental entities. Private entities provide external reporting to banks and other third parties in order to raise capital or meet contractual obligations. Not-for-profit entities prepare financial reports for donors, government agencies or other third parties. These external reports may be prepared in accordance with generally accepted accounting principles (GAAP) but may also be prepared in accordance with contracts and agreements, third-party preference or frameworks established by taxing authorities or regulatory agencies. Likewise, management's assessment of its internal control system may be made against criteria other than the COSO framework, such as those established by regulators, standard-setting bodies or other third parties.

The 1992 framework limited the reporting objective to an internal control system relating to preparation of reliable published financial statements. The 2013 framework continues to meet the needs of external published reporting but also encompasses the internal control requirements of reliable internal and nonfinancial reporting.

This paper focuses on management's assessment of ICEFR using COSO's updated 2013 framework.

Significant Changes Affecting Internal Control over Financial Reporting

The framework continues to address three objectives common to virtually all entities: operating objectives (pertaining to the efficiency and effectiveness of operations), reporting objectives (pertaining to the reliability of external and internal reporting) and compliance objectives (pertaining to compliance with applicable laws and regulations). Recognizing that the framework was used extensively to comply with SOX, which was issued subsequent to the 1992 COSO framework, COSO significantly expanded its discussion of internal control deficiencies in the 2013 edition, including tools to assist in deficiency evaluation. The scope of guidance applicable to larger companies, in particular, has been expanded. Discussion regarding technology, its infrastructure, development, use and links with other processes has been significanly enhanced to consider developments in these areas since 1992. Also considered with the 2013 edition are increased global regulations, such as environmental standards, and the growth of complex, interconnected business structures and management models, including outsourced operations.

The COSO framework continues to provide a common vocabulary for organizations to meet operational, compliance and financial reporting objectives.

Internal Control over External Financial Reporting (ICEFR) – 2013

Overview

Management establishes external reporting objectives to obtain reasonable assurance regarding the reliability of the published financial statements. From there, management develops sub-objectives to the level of detail where specific risks of material misstatement and omission can be identified. Sub-objectives must be specific, measurable or observable, attainable, relevant and time-bound. These include objectives over all processes relevant to significant financial transaction processing, including, for example, general ledger close and information technology, based on management's assessment of materiality. Often, sub-objectives are developed at the division, subsidiary, operating unit and functional or activity level. When specifying suitable external reporting objectives related to the preparation of external financial statements, management considers accounting standards, financial statement assertions and disclosure requirements.

The guidance on external financial reporting has warranted its own COSO publication, *"Internal Control over External Financial Reporting: A Compendium of Approaches and Examples*" (the compendium). This framework companion document includes the principles related to each of the five components, key considerations when determining how to meet the principles (Points of Focus), approaches to meeting the principles and real-world illustrative examples specific to ICEFR. With the compendium available for those users interested in ICEFR, COSO's core publication, *"Framework and Appendices,"* focuses the updated framework more broadly on operations, compliance and other reporting objectives.

The COSO tools no longer include example objectives for significant entity *activities*, risks to their achievement and control activities to address the risk. Instead, specific to ICEFR, COSO has greatly expanded approaches and examples to meeting the principles; however, these approaches and examples are in a generic form not addressing specific activity-level processes. One could say that although the guidance provided by COSO has increased, so has the requirement to use management judgment when selecting controls at the activity level.

Interrelationships Between Objectives, Components & Principles

Under the framework, controls are selected and deployed to effect one or more principles within each of the five components: Control Environment, Risk Assessment, Control Activities, Information & Communication and Monitoring Activities. All five components are pervasive, affecting the other four components, and are required for an effectively designed internal control system.

A system of internal control supporting the external financial reporting (*e.g.*, SOX 404) objective under the framework must include the five interrelated components and achieve the 17 principles to be designed and operating effectively—as is the case with any objective (operating, compliance or reporting) evaluated under the framework. In other words, when the components and principles are operating together in an integrated manner, they collectively reduce the risk of not achieving an objective to an acceptable level. The level of risk considered acceptable is a decision made by management based on the entity's risk tolerance.

Table No. 1 provides an overview of the framework's internal control components and the number of mandatory principles for each.

Table No. 1

Mandatory Internal Control Component	# of Mandatory Principles
1 – Control Environment	5
2 – Risk Assessment	4
3 – Control Activities	3
4 – Information & Communication	3
5 – Monitoring Activities	2

Principles are the fundamental concepts associated with the five interrelated COSO components. A principle not met under one component may directly affect the functioning of a principle in another component. Due to the interrelationships between the components, a nonexistent or nonfunctioning principle under one component has a pervasive effect on the other components. In other words, when one component is not present and functioning, all components cannot be present and functioning in an integrated manner, meaning the design and operating effectiveness of the internal control system as a whole is affected.

Consider Exhibit No. 1, for example. Principle 2 is one of the five principles required to be present and functioning for the Control Environment component to be present and functioning. However, the absence of Principle 2 may directly affect Principle 12 , affecting the Control Environment as well as the Control Activities component and the internal control system as a whole.

Exhibit 1

Component Name	Principle
Control Environment	#2: The board of directors demonstrates independence from management and exercises oversight for the development and performance of internal control.
Control Activities	#12: The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Further Discussion: Consider the situation where Principle 2 under Control Environment is not met and the board of directors does not demonstrate independence from management or exercise oversight for the development and performance of internal control. In this case, the entity has an increased risk that control policies and procedures, although in place and put into action, will be determined ineffective. In other words, due to the entity's failure to meet Principle 2, the risk of management override may preclude Principle 12 from being met as well.

Interrelationships Between Principles, Approaches & Points of Focus

Management selects and develops controls within each component to effect relevant principles—or in other words, to mitigate the risk the principle isn't present and functioning. COSO's approaches are example means to affect the principle. Likewise, COSO's Points of Focus are guidelines for entities to reveal risks by highlighting important characteristics relating to each principle. For example, the Points of Focus may reveal risks when management asks the question, "What is the risk to my organization if this Point of Focus were not in place and working at my organization?" The framework does not require management to assess separately whether the Points of Focus are in place.

ICEFR requires all five COSO components. Components support the functioning of other components and must work together in an integrated manner. The definition of internal conrol, unchanged from the 1992 framework, is a process, effected by an entity's board of directos, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

COSO Components in Depth

Control Environment

A properly designed and operating control environment is considered by many the most important component of an effective internal control system, due primarily to the pervasive impact on all other components that a control deficiency in this component could have (the impact partially demonstrated in Exhibit 1). The risks of management override and material financial statement omission or misstatement (including omissions and misstatements due to fraud, illegal acts and corruption) are control environment risks. As seen in Table 1, the control environment component is assigned the greatest number of mandatory principles to be met.

The definition and principles related to control environment remain virtually unchanged from the 1992 framework. Control environment encompasses the governance activities and ethical tone of individuals at the top of the organization, including the board of directors. The control environment includes the process of managing risk through oversight responsibilities, appropriate assignment of responsibilities and performance accountability.

Control Environment Component	
Principle Number	Principle Description
1	Demonstrate commitment to integrity and ethical values.
2	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	Demonstrate commitment to attract, develop and retain competent individuals in alignment with objectives.
5	Hold individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

Objective Setting – Overview

Risk assessment begins with management defining strategic and operational objectives. The objective-setting process is a prerequisite to developing an effective internal control system. Management establishes the entity's high-level objectives and sub-objectives to support the entity's mission, vision and strategies. Entity objectives and sub-objectives are designated as compliance, operations or reporting objectives and may relate to one, two or all three of those categories. A sub-objective in one category, such as timely compliance reporting, may support more than one objective. In this case, for example, a sub-objective of timely compliance reporting will support

both the reporting and compliance objectives. Objectives should be specified with sufficient clarity to identify and assess risks related to the objectives.

Risk Analysis – Overview

After objectives are established, an entity identifies and assesses risks to achievement of those objectives. Management uses the COSO principles to identify risks to meeting the objectives by asking, "What would be the specific consequences to my operating, compliance and reporting objectives and sub-objectives if this principle were not met?"

Once risks to achieving objectives (and sub-objectives) are identified (including the risk of fraud), management analyzes and evaluates their impact and likelihood of occuring against the entity's defined risk tolerances. Risks are then either accepted, transferred or managed with internal controls in accordance with those risk tolerances. Due to ever-changing internal and external environmental factors, the risk assessment process is a comprehensive, ongoing and changing process.

The underlying attestation process under SOX is not expected to change. To provide specific SOX compliance guidance, COSO's document "Internal Control over External Financial Reporitng: Compendium of Approaches and Examples" links the general principles included in the updated framework to approaches and examples relevant to preparing financial statements for external purposes.

Objective Setting – ICEFR

An ICEFR system is in place to reduce the risk to achieving an entity's objectives specific to external financial reporting. These objectives relate to the accounting standards appropriate for the entity and the assertions contained within them, such as the existence and completeness of transactions. Management should then further clarify external financial reporting objectives, *e.g.*, "Reliable financial statements reflecting complete and accurate financial statements in accordance with generally accepted accounting principles," into more detailed sub-objectives containing relevant assertions, *e.g.*, "Sales transactions are recorded in the correct period at the accurate amount for all services rendered."

Risk Analysis – ICEFR

Conducting a high-level risk assessment for ICEFR is the process of identifying the risks of not preventing or detecting, in a timely manner, a material omission within or misstatement of the entity's financial statements. When identifying the risk of material omission or misstatement, entities should consider the potential for fraud, including misappropriation of assets, fraudulent financial reporting caused by an intentional act, including management override of internal controls, and illegal acts and corruption.

Sub-objectives should include sufficient detail to identify where specific risks to meeting the objective are analyzed. Using the sales transaction recording example from above, risks would be worded based on the assertions contained within the control sub-objectives. For example, one risk to the sub-objective *"Sales transactions are recorded in the correct period at the accurate amount for all services rendered"* might be worded as *"Processes are not in place to prevent or detect improper cutoff of services rendered (and billed) at the end of a period, resulting in inaccurate recording of revenue."*

For external financial reporting objectives, risk acceptance should occur only when identified risks could not, individually or in the aggregate, exceed the risk threshold and result in a material omission or misstatement of the financial statements.

Risk Assessment Component	
Principle Number	Principle Description
6	Specify objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7	Identify risks to the achievement of its objectives across the entity and analyze risks as a basis for determining how the risks should be managed.
8	Consider the potential for fraud in assessing risks to the achievement of objectives.
9	Identify and assess changes that could significantly impact the system of internal control.

Control Activities

Management uses control activities to manage risks not accepted or transferred. A single control may affect multiple principles and support the achievement of multiple components, which in turn may support multiple control objectives or sub-objectives. Recognizing this, COSO has not tied the approaches in the updated framework to any one *activity,* such as Process Accounts Payable. This differs from the 1992 framework, where control activities are tied to specific risks, which are then in turn tied to specific activity-level control objectives. Although the framework principles are mandatory, COSO intentionally does not prescribe specific requirements of control activities that must be in place. Instead, management is encouraged to select, develop and deploy the controls for an effective internal control system based on factors unique to the entity and using the COSO-provided approaches and examples to apply the principle. Continuing with the example above regarding sales service transactions, a control activity to mitigate the specified risk associated with the sub-objective *"Sales transactions are recorded in the correct period at the accurate amount for all services rendered"* may be *"Services rendered are reconciled to services billed at the end of each period."*

The COSO publication for ICEFR, "Internal Control over External Financial Reporting: A Compendium of Approaches and Examples," provides approaches to meet the principles and real-world examples specific to external financial reporting.

Control Activities – ICEFR

Control activities over ICEFR are the actions directed by management, including the board of directors, to mitigate the risks of material misstatement or omission for external reporting objectives and sub-objectives. Control activities generally are deployed through policies that establish what is expected and procedures that put policies into action. Control activities are the responsibility of all levels of the entity, can be preventive or detective, automated through the use of technology or manual and include identifying and segregating incompatible functions to reduce to an acceptable level the risk of material error or omission, including fraud.

Management's process of selecting and developing relevant control activities begins with establishing financial statement materiality. Materiality sets the threshhold for determining whether a financial statement amount or disclosure is significant to the ICEFR assessment. Management then identifies the processes underlying significant financial statement amounts and disclosures. Significant transaction processes can be either manual or entail the use of computer application systems (including end-user computer applications such as spreadsheets)—or, as often is the case, a combination of the two.

Automated technology controls often are identified when computer applications are used to process significant transactions and disclosure amounts. Information technology general controls (ITGCs) are those IT controls upon which automated technology control activities rely to ensure the completeness, accuracy and availability of processing. Considering entity-specific factors and IT infrastructure complexity, ITGCs may include such items as access controls and controls over the acquisition, development and maintenance of technology and its infrastructure, including software version and patch management.

Management is responsible for the input, processing and output controls applicable to in-scope software applications, whether the application and its IT infrastructure are handled in-house or outsourced to a third party. In-house software application controls include controls over the development and maintenance of end-user computing applications, such as spreadsheets.

In addition to controls over significant transaction processing, including automated controls and ITGCs, ICEFR control activities generally also include controls over the general ledger close process, disclosures and significant accounting estimates.

In summary, management's assessment of controls should relate to their effectiveness in capturing and processing data about financial transactions from transaction initiation through authorization, recording, processing and, ultimately, reporting. Management judgment is a key element in selecting the best controls and ensuring they operate as designed. Controls are selected considering many factors, including the assessed risk of material omission and misstatement, evaluation of benefits and costs of designing and conducting effective controls (including segregation of duties and considering alternative preventive or detective controls), technology versus manual controls and the competency of personnel performing the controls.

Control Activities Component	
Principle Number	Principle Description
10	Select and develop control activities that contribute to the mitigation of risks to the achievement of objectives and acceptable levels.
11	Select and develop general control activities over technology to support the achievement of objectives.
12	Deploy control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

The Information and Communication component is highly integrated with the other four COSO components. For example, internally generated or externally gathered information supports the Risk Assessment component. Establishing and communicating a whistle-blower program often is an essential part of an entity's oversight of internal control activities and supports the Control Environment component. The Control Environment component simply cannot be performed and assessed without reliable information communicated timely to the right individuals, including an entity's board of directors.

Since SOX, external financial reporting and external internal control reporting go hand in hand. An entity's Information and Communication component therefore should be aligned to management's responsibilities for external financial reporting and monitoring the internal control system. Individuals identify, gather and classify the pertinent information (both for financial reporting and internal control) and communicate to individuals

responsible for external financial reporting. Entities commonly use data flow diagrams, flowcharts, narratives and procedure manuals to document the flow of information and accountable parties.

SOX is an example where the Information and Communication component encompasses communicating internally generated information to external regulatory agencies, stakeholders and third-party business partners, *e.g.*, contractors and customers. Information and Communication also goes the other way and includes gathering pertinent information from external regulatory bodies and other sources to prepare, *e.g.*, accounting estimates.

Information & Communication Component	
Principle Number	Principle Description
13	Obtain or generate and use relevant, quality information to support the functioning of internal control.
14	Internally communicate information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15	Communicate with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

The initial design of the internal control system becomes an entity's baseline for future monitoring of the system. The controls within other components of the framework require continuous monitoring—either as ongoing evaluations, separate evaluations or a combination of the two. Assessments can be conducted by the individuals performing the control (self-assessments) or by independent internal or external third parties. Although an external financial statement audit may reveal certain items about an entity's internal control system, an audit should not be relied upon to evaluate the effectiveness of an entity's internal control design or operating effectiveness or to provide feedback on such.

Controls are used to implement principles within each component of the framework, including the monitoring component. Changes in the internal and external business environment, including technology, require re-evaluation of control objectives, risks to meeting those objectives and relevancy and sufficiency of controls.

Metrics often are used as a monitoring activity to determine whether internal controls over financial reporting are designed properly and operating as designed. For example, to determine whether financial transactions are completely and accurately reflected in the financial statements, an entity may compare payroll to prior periods, or the average number of employees, or operating information. Certain entities monitor controls through the use of automated monitoring applications, which can be programmed to identify anomalies or track patterns and trends. This information often leads to process improvements.

Monitoring Component	
Principle Number	Principle Description
16	Select, develop and perform ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17	Evaluate and communicate 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.

Assessment of a System of Internal Control & Deficiencies

COSO has clarified the requirements for effective internal control. An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective or objectives. In determining whether an overall system of internal control is efffective, senior management and the board of directors assess whether each of the five components and relevant principles are present and functioning and whether the components operate together in an integrated manner. The existence of a major deficiency precludes an organization from concluding it has met the requirements for an effective system of internal control under the framework.

Regarding the evaluation of ICEFR, the 2013 framework is more prescriptive. For effective internal control, the framework presumes all 17 principles are present and functioning. In other words, if a principle is not present and functioning, the associated component is not present and functioning. If management determines a principle is not relevant, management must be able to support that determination, as well as how, in the absence of that principle, the associated component can be present and functioning.

Deficiency Defined

The framework defines an internal control deficiency as a shortcoming in one or more components and relevant principle that reduces the likelihood that an entity can achieve its objectives. The framework requires management to use judgment to assess the severity of that deficiency in determining whether the relevant principle and component are present and functioning. If, in management's judgment, a control deficiency severely reduces the likelihood that the entity can achieve its objectives, then it is defined as a major deficiency under the framework. If a major deficiency exists, management would conclude that the component is not present and functioning and the system of internal control is not effective.

The Financial Accounting Standards Board (FASB) and other regulators and accounting standard setters establish laws, rules, regulations and standards relating to the preparation of financial statements for external purposes. Regulators and other standard setters also establish criteria for defining the severity of, evaluating and reporting internal control deficiencies. An entity reporting to a third-party standard setter should use the criteria established by the regulator, standard-setting body or management and the board of directors when classifying the severity of internal control deficiencies, rather than the classification set out in the framework.

COSO's definition of a deficiency, for example, differs from that set out by the SEC. For those entities that must comply with the SEC regulations, the entity would classify a deficiency as a material weakness, significant deficiency or control deficiency (as pertaining to financial reporting) in accordance with the criteria established by the SEC. Management would in turn assess any material weakness, significant deficiency or control deficiency identified under the SEC criteria to determine its impact on the relevant principle(s) of internal control contained within the framework.

An entity evaluating a deficiency based on criteria established by a regulator or standard-setting body must use that criteria when classifying the severity of internal control deficiences. If a deficiency is determined to rise to the level of a material weaknesss, the entity would not be able to conclude that the entity's system of ICEFR has met the requirements for effective internal control as set out in the Framework. Conversely, if the internal control deficiency does not rise to the level of material weakness the entity could achieve effective ICEFR.

The templates in COSO's *"Illustrative Tools for Assessing Effectiveness of a System of Internal Control*" were significantly enhanced from the 1992 *"Evaluation Tools"* to provide guidance on performing an overall assessment of a system of internal control. The optional risk-based templates provide tiered guidance, beginning with evaluating whether each principle is functioning and present through evaluation of whether the component is functioning and present and ending with a template for overall assessment of the system of internal control. Documentation of the evaluation of deficiencies is emphasized, focusing on evaluating the severity of deficiencies and including consideration of how deficiencies related to different principles could affect one another.

The framework continues to include a principle specific to evaluating and communicating internal control deficiencies, which must be met for management to conclude the internal control system is designed and operating effectively.

Transition

Transition brings with it new challenges. Both the 2013 and 1992 frameworks are available until December 15, 2014, and management must describe which framework it is using for its assessment. Using accounting standard setter language, the transition is prospective.

When looking at SOX compliance, a couple of items should be considered. First, internal controls need to be in place for a reasonable period of time. Second, management is expected to obtain persuasive evidence to support its determination that the internal control system is present and functioning. Management's assessment should include review of both of the following:

- Evidence of the design of the internal control system considering changes in the business
- Evidence the internal control system is operating as designed, including tests over system-generated data and reports and updated testing of controls from interim to year-end (if controls were tested at an interim period)

Recent communications from the SEC indicate it plans to monitor the transition for issuers currently using the 1992 framework to determine whether any staff or commission actions—including setting a specific transition period—become necessary or appropriate at some point in the future. The current view is that SEC staff will allow issuers to continue using the 1992 framework for a period of time beyond COSO's transition date; however, the longer issuers continue to use the 1992 framework, the more likely it will be that questions from the SEC will arise. SEC Chief Accountant Paul Beswick reiterated COSO's statements that users should transition their applications and related documentation to the the 2013 framework as soon as feasible under their particular circumstances, but that the 1992 framework's principles and concepts are still sound and accepted during the transition period.

COSO's 2006 publication, "Internal Control over Financial Reporting – Guidance for Smaller Public Companies," still is available to provide guidance for smaller public companies in how to apply the framework to efficiently comply with Section 404. Note, however, the principles underlying components of internal control are just as applicable for smaller entities as for larger ones. The implementation approaches for smaller entities may differ.

Management should begin assessing whether the 17 principles are relevant to their organization and are present and functioning. Entities should map existing controls to relevant principles within each component and perform a gap analysis—identifying where controls do not exist to mitigate the risk to meeting the principle (and related objectives and sub-objectives) to an acceptable level. Management would then establish a process for identifying, assessing and implementing necessary changes in controls and related documentation. This would not be performed in a silo. Management will generally need to engage resources from across functions and territories to adopt the 2013 framework and make the necessary changes. The effort required to transition will depend to a certain extent on how well the entity understood and applied the key concepts and principles contained in the original framework.

Conclusion

The 2013 COSO framework is a must-read for all boards and managers. The principles-based framework can be adopted to an internal control system of any type of entity, regardless of size, industry or structure. To properly evaluate a system of internal control, components and their principles should be evaluated together. This will require input from new hires to experienced executive managers and will encompass operations, compliance and reporting functions alike.

COSO considers the 1992 framework superseded as of December 15, 2014, but there are other reasons to look at internal controls from a fresh perspective, such as increased risk resulting from changes in markets or products, increased regulatory oversight and compliance requirements, greater reliance on ever-changing technology and increased operating structure complexity with greater roles for third-party relationships/service providers and continued corporate restructuring, mergers and acquisitions. The updated framework may be the push organizations need to reassess existing controls in relation to the risks of achieving objectives.

COSO framework users should continue monitoring guidance from appropriate regulators and standard setters following the issuance of the updated framework. If you have any questions, please contact your BKD advisor.

Contributor

Connie Spinelli
Director
303.861.4545
cspinelli@bkd.com