Present and functioning: Fine-tuning your ICFR using the COSO update

November 2014

With the COSO's 1992 Control Framework being superseded by the 2013 updated edition on December 15, 2014, now is the time for companies to use the updated framework to evaluate the effectiveness of their systems of internal control over financial reporting.

Introduction

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published *Internal Control—Integrated Framework*, which gave organizations guidance for designing, operating, and evaluating their systems of internal control over financial reporting (ICFR). That publication will be superseded by an updated edition on December 15, 2014, and many US public companies are already well on their way to transitioning—a process made easier by the fact that the core concepts for effective ICFR are not fundamentally different from those set forth in the original edition. The updated framework formalizes 17 principles that stipulate more-granular evaluative criteria to help a company's management assess the design and operating effectiveness of its ICFR. And to meet the requirement that calls for evaluation of whether each principle is present and functioning, senior managers at leading companies are taking a fresh look at how their existing controls support the 17 principles.

For more than 20 years, the original COSO framework has helped management design, operate, and evaluate the effectiveness of its ICFR, and it has provided reasonable assurance of the reduction of the risk of material misstatement to an acceptable level. The largest component of effective ICFR covers control activities. These controls—in the forms of transaction-level controls and review controls in business processes—typically represent 85 to 95% of a company's ICFR. Also, transaction-level controls and review controls are intended to have a direct effect on the likelihood that a misstatement will be prevented or detected and corrected on a timely basis. We don't believe that implementation of the 2013 framework affects management's existing control activities. In fact, the 2013 framework prescribes no specific control activities, and the formalization of the three principles related to control activities does not change the requirements regarding their design and operation. Therefore, assuming that a company's control activities have been assessed as effective, reevaluating them according to the 2013 framework is not necessary.

We believe the most immediate value of applying the 2013 framework lies in the opportunity it provides for taking a fresh look at indirect entity-level controls (ELCs)—which are controls that have both an important effect on ICFR and an indirect effect on the likelihood that a misstatement will be prevented or detected and corrected on a timely basis. These controls are important for support of the principles in the so-called softer components of internal control, namely: control environment, risk assessment, information and communication, and monitoring activities.

> **This publication identifies opportunities to fine-tune the design and related documentation of indirect ELCs through mapping them to principles within those softer components. It also covers challenges in evaluating the design and operation of those controls.**

COSO principles

The 2014 COSO framework sets out 17 principles that represent the fundamental concepts associated with each component of internal control.

Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information and communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Fine-tuning for effectiveness and efficiency: Addressing the principles

In our experience with companies that are implementing the 2013 framework to evaluate the design and operation of their indirect ELCs that are important to ICFR, we have noted the following areas in which management's assessment has indicated room for optimization or improvement in control documentation.

Principle 4: The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives

Leading companies are formalizing or clarifying and incorporating into their evaluations of ICFR certain indirect ELCs that support existing human resources policies. Such controls usually consist of approvals of new hires and employee transfers (including background checks and assessments of requisite skills and experience when appropriate), requirements for professional certifications and training (e.g., in new and complex accounting standards), succession planning and retention of competent employees, and periodic reviews of employee performance to assess requisite skill levels and conduct. Compensation programs aligned with expected performance, competencies, and behaviors are also important to support ICFR objectives.

Principle 8: The organization considers the potential for fraud in assessing risks to the achievement of objectives

In many organizations, the evaluation of fraud risks related to financial reporting is integrated into the overall assessment of financial-reporting risks. Leading companies establish accountability for indirect ELCs that assess fraud risk scenarios relevant to the organizations and their respective industries and geographic regions. Fraud risk scenarios might include material bias in the development of complex accounting estimates, the overriding of controls in stuffing inventory into distribution channels to manipulate revenue recognition, and noncompliance with the Foreign Corrupt Practices Act.

In identifying and evaluating those risks, management investigates incentives, pressures, opportunities, attitudes, and rationalizations that might exist throughout the company in different departments and among various personnel. This undertaking equips management to determine the mitigating actions it should take to reduce to acceptable levels any risks of material misstatement due to fraud.

Fraud risk assessment should benefit from the active involvement of management with sufficient knowledge of the business and who are at the right levels throughout the organization. Such involvement might include conducting workshops and holding brainstorming sessions designed to identify and assess risks of material misstatement due to fraud organization-wide. Fraud risk assessment should be updated periodically by considering external and internal changes during the reporting period that could affect previous conclusions. Reasonable supporting documentation of this risk assessment is retained, along with documentation detailing the audit committee's involvement and oversight.

Principle 9: The organization identifies and assesses changes that could significantly impact the system of internal control

Depending on the nature of the change, the responsibilities for identifying, evaluating, and responding to changes in the business that are likely to have a material impact on financial reporting are usually spread widely across the organization. Leading companies establish accountability for indirect ELCs designed to identify and assess changes during the current reporting period that could affect the company's previous assessment of the risks of material misstatement. Such changes generally include new accounting standards; new business transactions, events, or conditions (or changes in existing ones); and important changes in the business processes, information systems and communications, and personnel that support key control activities. Those controls focus on assessing the impact of such changes on previously assessed risks of material misstatement. The identification and assessment process enables management to determine the mitigating actions necessary to reduce to acceptable levels the risks posed by such changes—primarily through alterations in the design and operation of control activities. Financial-reporting risk assessments are reviewed periodically by those who possess the necessary skills and experience—both in the business and in financial reporting and ICFR—for conducting a thoughtful review.

Principle 13: The organization obtains or generates and uses relevant, quality information to support the functioning of internal control

Because control activities depend on having reliable information and data, companies must assess changes in business processes and information systems to make sure that only reliable information and data continue to be used in the operation of those controls. The 2013 framework does not require companies to do anything differently from before. For example, companies use IT change controls over system development and application controls in automated information systems to confirm whether packaged and customized system-generated reports contain reliable information for application in control activities. Control activities also must be in place to obtain reliable information from queries of automated information systems, end-user spreadsheet applications, and external and internal sources when IT general controls and application controls cannot be used.

Challenges in evaluating and testing indirect ELCs

Leading companies can use the principles to deliver more clarity in the design of indirect ELCs that support the principles within the softer components of internal control and thereby possibly attain greater assurance in their ICFR. Following are several of the more challenging aspects of determining what's important for demonstration that a principle is present and functioning throughout the company in an ICFR context.

Distinguishing programs, processes, and practices from controls

It can be difficult to distinguish programs, processes, and practices—which ordinarily describe ongoing tasks and activities—from controls, which are meant to establish or implement a policy or procedure for providing reasonable support that a principle is present and functioning. More specifically, the deployment of indirect ELCs is important for demonstrating that principles in the softer components of internal control are present and functioning. For example, a company might have a required accounting training program to support principle 4, whereas an indirect ELC can determine whether designated personnel completed the training program *and* can ensure that appropriate follow-up actions are taken. Inadequately distinguishing between the two could result in (1) less-effective controls supporting management's assessment of ICFR or (2) unnecessary evaluations of programs, processes, and practices.

Distinguishing ELCs that support ICFR from non-ICFR objectives

Companies don't always tell the differences between ELCs that support ICFR and those that support non-ICFR objectives. It's important to focus on ELCs that enable management to demonstrate that a principle is present and functioning in an ICFR context. To the extent that an ELC is irrelevant to—or has only limited relevance to—financial reporting, that ELC does not need to be considered. However, an ELC that is designed to support both ICFR and non-ICFR objectives is considered. For example, if an indirect ELC supports the audit committee's oversight of multiple company-wide objectives (e.g., ICFR and other regulatory compliance reporting), it's important that the control objective(s) and procedure(s) specifically address *how* oversight is exercised over ICFR.

As another example, consider the following ELCs—embedded in a whistle-blower hotline program—which support ICFR and other objectives.

ELC 1	Incidents that could affect financial statements are tracked, investigated, and acted upon in a timely manner by the chief compliance officer.
ELC 2	The chief compliance officer submits quarterly reports to the audit committee on all issues that could affect the financial statements.
ELC 3	Incidents that involve human resources matters (e.g., age discrimination) are tracked, investigated, and acted upon by the head of human resources in consultation with the office of general counsel.

ELC 1 and ELC 2 are relevant to ICFR because they're expected to have a pervasive effect throughout the company on control activities designed to prevent or detect material misstatements. ELC 3, however, probably would not result in a risk of material misstatement and therefore would not be relevant to ICFR.

Similarly, an indirect ELC embedded in *management's* risk assessment process could consider the *company's* enterprise risk assessment so that management can identify changes in the business that might affect financial reporting and ICFR (principle 9). If so, management's risk assessment would focus on assessing only those business issues that introduce new—or that affect previously assessed—risks of material misstatement.

Distinguishing indirect from direct ELCs

Companies are becoming more adept at telling the differences between various types of ELCs. For example, direct ELCs such as business performance reviews are designed with a level of precision that can directly affect the likelihood that a material misstatement in the financial statements will be prevented or detected and corrected on a timely basis. For that reason, *direct ELCs* can be considered compensating controls in evaluating—and reducing—the severity of deficiencies in other control activities. *Indirect ELCs* have an important impact on the design and operation of control activities but are not designed to operate at a level of precision that can prevent or detect and correct on a timely basis a material misstatement in the financial statements.

Distinguishing design effectiveness and extent of testing for indirect ELCs versus control activities

Companies are not always certain what kind of evidence constitutes reasonable support for the design and operation of indirect ELCs. It's important that design documentation clearly describe the objectives, the procedures, the qualified personnel responsible, and the frequency of occurrence or triggers. Leading companies are taking a fresh look at indirect ELCs to ascertain which ones are important for making effective and efficient determinations of whether a principle is present and functioning throughout the company in an ICFR context. Many are reevaluating whether the control objectives and procedures align closely with a principle in an ICFR context, whether qualified individuals are responsible for reevaluating control design throughout the company if necessary, and what condition or event would trigger operation of the control or how frequently the control would operate if it's on a regular, recurring schedule.

Certain outputs of indirect ELCs such as management's review of the fraud risk assessment, as discussed earlier, might benefit from taking a fresh look at the operation of those controls. In addition, management is recognizing that the nature and extent of testing *indirect ELCs* for operating effectiveness are not the same as what's necessary for testing *control activities*. This is due to the difference between the *objectives of indirect ELCs* and the *objectives of control activities*—including direct ELCs, as described in the previous section.

Evaluating controls at outsourced service providers

Management is ultimately responsible for the design and operation of its ICFR, including the controls that are designed and operated by outsourced service providers. With some service providers, companies can find it challenging to obtain an understanding of those controls, evaluate them, and conduct adequate testing. To that end, leading companies usually have in place:

- *An indirect ELC to inventory existing outsourced service providers and service-level arrangements* that have a significant impact on the company's ICFR.
- *An indirect ELC to evaluate and select vendors* with competencies in financial reporting and ICFR, such as the ability to satisfy the service requirements specified in a service-level agreement (e.g., code of conduct, IT and financial-reporting standards and guidance, quality and timeliness of reporting and communication, skills and experience). Vendor selection depends on completion of an initial assessment of financial-reporting risks and a determination of the responses necessary to mitigate such risks to acceptable levels—such as through contractual provisions that require a Service Organization Control (SOC) 1 audit report on internal control and/or separate evaluations of controls at the service provider.
- *An indirect ELC to periodically evaluate the performance of service providers* against criteria set out in service requirements relevant to ICFR and to update financial-reporting risk assessments and responses in reporting periods after the initial assessment.
- *An indirect ELC to review a SOC 1 report* and determine whether any follow-up actions are necessary.
- *Control activities* (including direct ELCs) to verify the reliability of data and information—relevant to the company's ICFR—that are sent to and received from service providers.

Identifying financial-reporting risks related to operations, nonfinancial reporting, and compliance

Management's financial-reporting risk assessment and the underlying indirect ELCs must consider the risks of material misstatements that might be attributed to control deficiencies in the company's operations, nonfinancial reporting, and compliance. For example, the risk assessment would have to consider the likelihood of a material misstatement in connection with an ongoing dispute with a third party, the quality of production issues, or incomplete or inaccurate regulatory filings.

Management might also have to evaluate non-ICFR controls that are supporting the generation of nonfinancial information used in control activities that support financial reporting and ICFR. For example, the results of a customer survey could be used to inform or support the development of accounting estimates underlying the company's accrued warranty costs.

Documenting management's consideration of financial statement assertions

Management's assessment of financial-reporting risks focuses on material accounts and disclosures in the company's financial statements. Management explicitly or implicitly makes assertions (e.g., regarding completeness, accuracy, or validity) about the significant accounts and disclosures. Therefore, management's risk assessment typically includes assessments of financial-reporting risks for assertions that are relevant to material accounts and disclosures. Previous risk assessments provided the basis for designing and operating control activities (such as transaction-level controls and review controls) to mitigate such risks of material misstatement throughout the company. When management updates those previous risk assessments for changes in the business (e.g., new accounting standards, new business transactions) during the current reporting period, it continues to assess assertions relevant to material accounts and disclosures.

Mapping indirect ELCs to points of focus

The 2013 framework includes a series of points of focus that describe important characteristics of the principles. Those points are intended to help management design, operate, and evaluate the effectiveness of its ICFR. Management may find the points of focus helpful in identifying or describing certain indirect ELCs that are important for demonstrating that a principle is present and functioning in the company's ICFR. Organizations should keep in mind that the points of focus are guidances rather than requirements. For instance, the 2013 framework requires an evaluation as to whether *the 17 principles* are present and functioning, but it imposes no requirement to assess the presence or functioning of any of *the points of focus*.

Mapping indirect ELCs to multiple principles

Leading companies recognize that important indirect ELCs can support multiple principles in an ICFR context. For example, an indirect ELC in the whistle-blower hotline program can support both principle 1 and principle 14. Likewise, an indirect ELC related to internal communication between management and the audit committee about the company's financial-reporting policies and ICFR can support both principle 2 and principle 14.

Conclusion: Better ICFR—and beyond

With the advent of COSO's updated control framework, many leading companies are choosing to make the transition now. Those companies are taking advantage of the opportunity to reexamine the indirect ELCs that are important to the principles in the softer components of internal control: control environment, risk assessment, information and communication, and monitoring activities. Many are finding that those controls map rather well to the principles. They're also identifying additional indirect ELCs that are important for demonstrating a principle is present and functioning and that it should be included in their annual assessment of ICFR, as required by the Sarbanes-Oxley Act. And in alignment with the principles, they're clarifying the objectives, procedures, responsible personnel, and locations covered by those controls. Companies taking a thoughtful approach in transitioning to the 2013 framework—rather than viewing it as a mere compliance exercise—are finding value in the identification of opportunities to strengthen their ICFR.

Once a company has gone through the transition in connection with its annual ICFR assessment and has developed institutional knowledge, familiarity, and comfort with the principles, the next step is to use those competencies and apply the 2013 framework to other suitable entity objectives beyond ICFR such as complying with evolving environmental standards, managing technological change, optimizing management risk assessment processes that support important entity objectives, and achieving consistent control across global organizations with multiple operating models and legal entity structures. A forthcoming PwC publication will explore the potential application of the 2013 framework to those types of optimization and non-financial-reporting objectives.

www.pwc.com

Contacts

For a deeper discussion please contact:

Jason Pett
Internal Audit Leader
jason.pett@us.pwc.com

Kenneth Blomster
Risk Assurance Partner
kenneth.blomster@us.pwc.com