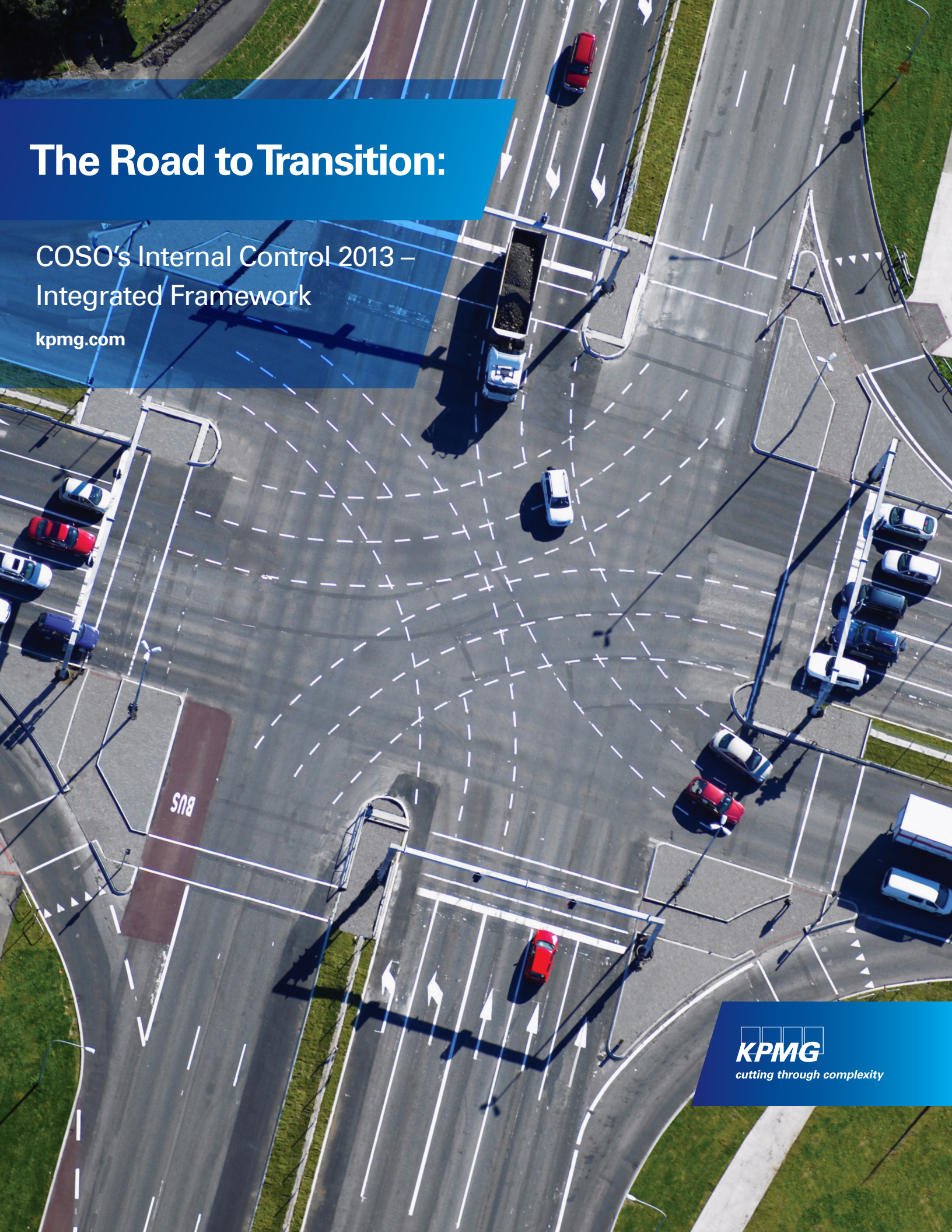
The Road to Transition:

COSO's Internal Control 2013 – Integrated Framework

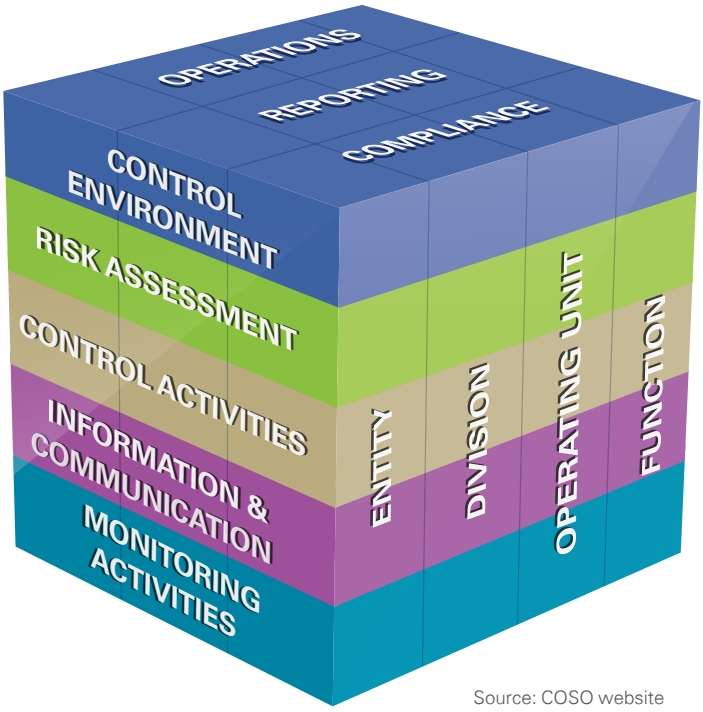
kpmg.com



KPMG
cutting through complexity

The Road to Transition:

COSO's Internal Control 2013 – Integrated Framework



Source: COSO website

Since its inception in 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s Internal Control — Integrated Framework has seen widespread acceptance in the design and evaluation of organizational internal control. Public companies and other entities globally use it to evaluate and document the effectiveness of their internal control systems, particularly those related to financial reporting (ICFR).

Recently, the COSO Board updated the framework to make it increasingly relevant for investors and shareholders amid a dynamic and rapidly evolving business environment. COSO's 2013 Framework is, thus, aimed at enhancing organizations' control structures within the context of a rapidly evolving business environment.

What has changed?

The changes made to update the 1992 Framework are evolutionary, not revolutionary. 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 each of the five components and the 17 relevant principles be present and functioning; and 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 system of internal control. These components, shown in the table below, along with their related principles, serve as comprehensive guidance for companies looking to strengthen their internal control systems.

The Five Components Functioning Together

When management evaluates control deficiencies identified as part of their assessment of the effectiveness of their internal control over financial reporting, the focus, in many instances, is solely on the severity of the identified deficiency within the control activity. If the five components of internal control are functioning together effectively, management should consider whether a deficiency also exists in one of the other components, e.g., control environment, risk assessment, information and communications or monitoring, depending on the severity and/or type of deficiency identified.

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 & 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

The new version also features the following changes from the 1992 Framework:

- Additional guidance on the role of technology in processes and reporting systems
- Increased insight into the concepts of governance
- Heightened focus on globalization and changing business models
- Expansion of the reporting objective to include internal and external financial and nonfinancial reporting
- Increased emphasis on assessing and responding to fraud risk and its relationship with internal control

Opportunity in change

As noted above, the most significant change in the updated framework was the codification of the 17 principles that were implicit in the 1992 Framework component. Assessing how 17 principles in the 2013 Framework apply to an organization offers an opportunity for management to "stand back" from its existing control structure to determine if (1) its internal control structure contains the required elements to mitigate the risks to the achievement of the objectives, and (2) whether changes to the system of internal control can, or should be, made to reflect changes in the business. These changes could arise from, for example, acquisitions, significant structural changes, or changes in information technology, including use of third-party providers.

Management can also use the 2013 Framework to evaluate whether changes can be made to improve the efficiency or effectiveness of the organization's system of internal controls. For example, the 2013 Framework provides an opportunity to further integrate existing risk and compliance functions to streamline processes and reduce costs.

For effective internal controls, the 2013 Framework requires that each of the five components and 17 relevant principles be present and functioning. In many cases organizations have focused most of their time and attention on identifying and documenting control activities for ICFR compliance. The 2013 Framework offers organizations an opportunity to re-evaluate the strength of the other internal control components—specifically risk assessment, monitoring, and information and communications—to determine if they are keeping pace with the evolving business environment and emerging risks.

The importance of all five components of an internal controls structure to an effective system of internal controls was reinforced in a speech by Brian Croteau, Deputy Chief Accountant, Office of the Chief Accountant U.S. Securities and Exchange Commission in which he discussed the upcoming release of the 2013 Framework. In his remarks before the 2012 AICPA National Conference on Current SEC and PCAOB Development he said: "Finally, I'd like to remind management and auditors of something that may sound quite obvious: COSO has five components. While evaluating the control activity component is very important, the control environment, risk assessment, monitoring, and information and communication components are important to an effective system of internal control in accordance with COSO's framework"

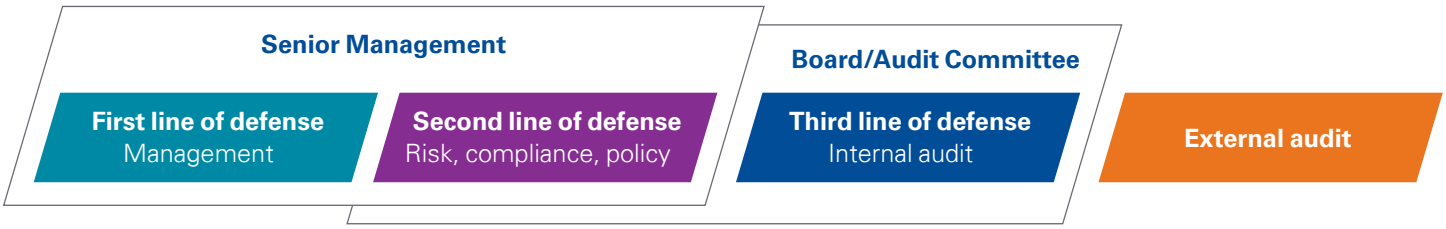
In addition to the above, according to COSO, the benefits that the 2013 Framework offers include the following:

- Enhanced governance
- Extended coverage/applicability for the reporting objective beyond financial reporting to other forms of reporting, operations, and compliance (for example, sustainability reporting)
- Improved risk assessment and antifraud practices
- Enhanced adaptability to change and varied business/operating models

As businesses evaluate the impact of the 2013 Framework on their internal control structure, stakeholder groups should consider their role in the assessment and transition with respect to their roles and responsibilities for internal control.

Preparing for the transition…

It is important that the three lines of defense—(a) management and senior management (b) risk, compliance and other policy setting groups and (c) internal audit—fully comprehend the implications of the updated framework. The purpose of evaluating the 2013 Framework is to understand where the relevant principles are present and how they support the control objectives established by management.



First and Second Lines of Defense

Prior to implementation, management should obtain an understanding of the updated framework's components, principles, and points of focus. Once there is an understanding, a detailed assessment should be completed to identify gaps between existing control structures and anticipated changes as a result of the 2013 Framework. Mapping the 17 principles, considering the points of focus, to either existing or anticipated controls is integral to understanding where the relevant principles are present, and how these support the control objectives and identifying weaknesses or gaps in internal control. As part of this assessment, management should assess if changes to the system of internal control can, or should be, made to reflect changes in the business.

Finally, management will need to adopt a transition plan to remediate identified gaps. The transition plan should include elements such as education and training for personnel on the 2013 Framework, mapping of the organizations' existing controls to the updated framework, identification of gaps and modifications needed to address the 2013 Framework, and steps to be taken to remediate gaps and make the necessary modifications.

Functional risk, compliance and policy-setting groups can play a critical role in assisting management with their understanding and assessment and work toward remediating gaps in control design as the transition evolves. In addition, these internal groups should make their own assessment and evaluate the need to update policies, guidance and tools to reflect the principles and points of focus. They should also work with management to communicate to Internal Audit and the Board/Audit Committee the results of their assessment and transition plans for remediating weaknesses identified.

Third Line of Defense

Internal Audit should also consider how the 2013 Framework impacts their existing processes. How will the internal audit planning process be modified to consider the principles within the 2013 Framework and the implications of changes in the business environment, business objectives and emerging risks to those principles and the overall internal control structure?

The Board/Audit Committee should understand how management is addressing the 2013 Framework and the timing and implications of migrating from the 1992 Framework to the 2013 Framework. In addition, it is important to engage in discussions with your external audit firm to review the organization's 2013 Framework transition plan and understand implications on the execution of the 2013 and 2014 audits.

In summary, the involvement of all three lines of defense and stakeholder groups is a prerequisite to successfully transition to the 2013 Framework and helping your organization achieve a system of internal control that is effective in a dynamic business environment.

Enterprise Risk Group

Assessing risk tolerance, risk velocity and risk persistence are more clearly articulated in the 2013 Framework than in the 1992 Framework. Risk groups may decide to update company guidance to include a discussion on risk tolerance, velocity and persistence for the organization as a whole as well as for significant components or processes

Table 1 – Actions to Consider

Stakeholder	Actions for Consideration
First Line of Defense – Senior Management	• Develop your plan to transition from the 1992 to the 2013 Framework. Your transition plan should consider: – Education on and evaluation of the 2013 Framework and its changes – Mapping of the existing system of internal control to the 2013 Framework – Assessment of the efficiency and effectiveness of the existing system of internal control – Implementation of new or upgraded controls, if needed – Interaction with the Audit Committee, Board, and external auditors – Evaluation of impacts on reporting (e.g., sustainability reporting and changes in internal control under Regulation S K, Item 308(c))
First Line of Defense – Line Management	• Map the 17 principles and points of focus to your existing controls or controls the organization is contemplating in an organizational transformation within each component to demonstrate where the relevant principles are present and functioning in support of the objectives. • Identify and discuss control design gaps with senior management and develop plans to remediate any such gaps.
Second Line of Defense – Risk, Compliance and Other Policy Setting Groups	• Perform an assessment of the impact of the 2013 Framework on your organization's policies, guidance, training and related tools. • Work with senior and line management to communicate the impact of the 2013 Framework on the organization to Internal Audit and the Board/Audit Committee.
Third Line of Defense – Internal Audit	• Discuss with the audit committee the impact of the 2013 Framework on Internal Audit's operations and plans. • Proactively work with first and second lines of defense to create and manage the transition process to the 2013 Framework
Third Line of Defense – Boards of Directors and Audit Committees	• Understand how management is addressing the 2013 Framework and the timing and implications of migrating from the 1992 Framework to the 2013 Framework. • Engage in discussions with your external audit firm to review the organization's 2013 Framework transition plan and understand implications on the execution of the 2013 and 2014 audits.

Questions to Consider

- Has my documented system of internal control kept pace with significant changes in my business organization, operations, technology and governance needs?
- Does my control structure create the flexibility needed to manage increased globalization, an increasing complex regulatory environment and rapidly changing technology and its impacts on my stakeholders?
- Do my risk assessment and monitoring controls function as an "early warning system" that act in unison with the other COSO objectives?

- Does my control structure reflect a cohesive approach to controls for my organizational unit or function?
- Does my control structure address the revised language of the reporting objective to cover internal and external financial and non financial reporting?
- Have I designed my risk assessment and monitoring controls in a way that is precise enough to manage the specific risks within my organizational unit or function?

- Has the organization defined and provided guidance on risk tolerance, risk velocity and persistence in a way that is readily understood within the organization?
- Has the organization taken full advantage of the use of monitoring controls, including data analytics, within its control structure to better monitor the effectiveness of process-level controls and identify process-level changes?
- Can we use the 2013 Framework to better integrate our compliance needs to lower costs and create a more transparent compliance process?

- Have we identified the potential impacts of the 2013 Framework on our audit methodology?
- Is there a focus on evaluating the clarity of business objectives such that significant risks to those objectives can be identified and assessed?
- Does the organization's and internal audit's risk assessments incorporate risk tolerance, velocity and persistence?
- Does our methodology actively assess whether controls are adapting to changing risk profiles or changing objectives?

- Has management's plan fully addressed all aspects of the changes to the 2013 Framework?
- Does management's transition plan appropriately account for the people, process and technology resources that will be needed for the transition?
- What changes does the external audit firm expect as a result of the 2013 Framework for your organization?

Contact us

Sam Fogleman
Partner
T: 313-230-3065
E: sfoglema@kpmg.com

Sue Townsen
Partner
T: 212-872-2178
E: stownsen@kpmg.com

Emad Bibawi
Partner
T: 212-954-2033
E: ebibawi@kpmg.com

kpmg.com