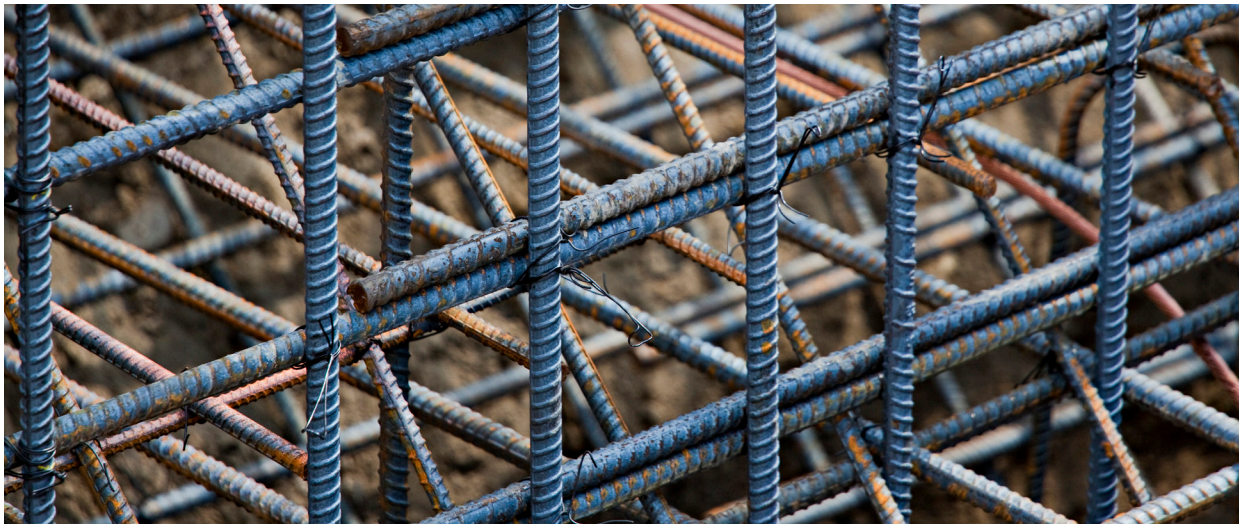
Deloitte.

Implementing the updated 2013 COSO framework: Takeaways for banking and capital markets firms



The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released an update to the *Internal Control – Integrated framework* (2013 COSO framework) in May 2013. Much has changed in the business, regulatory, and operating environment since the original 1992 framework was released. The updated framework continues its aim to assist organizations in their ongoing efforts to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving an organization's objectives.

The 2013 COSO framework retains the five components of internal control from the original framework, but introduces 17 principles that are associated with the five components. The principles are further supported by 87 points-of-focus, which provide additional guidance and clarity for designing, implementing, and maintaining a system of internal control and in assessing whether the 17 principles are present and functioning. The 2013 COSO framework presumes that because the 17 principles are fundamental concepts of the original five components, all 17 are relevant to all entities and need to be present, functioning, and operating together in an integrated manner for an organization to have an effective system of internal control.

COSO will continue to make the 1992 framework available until December 15, 2014, after which time it will consider it to be superseded. Companies applying and referencing COSO's internal control framework for purposes of complying with Section 404 of the Sarbanes-Oxley Act of 2002 (SOX 404) should consider COSO's transition guidance. Additionally, the U.S. Securities and Exchange Commission (SEC) has also indicated that "the longer issuers continue to use the 1992 framework, the more likely they are to receive questions from the staff about whether the issuer's use of the 1992 framework satisfies the SEC's requirement to use a suitable, recognized framework (particularly after December 15, 2014)…".[1] As the COSO framework is widely used to support management's assertion on the effectiveness of internal controls over financial reporting, and the possibility of significant effort necessary to meet the elevated expectations, companies should begin moving forward with urgency.

Experience gained from assisting banking and capital markets firms with 2013 COSO framework readiness assessments, as well as implementation of enhancements to current COSO programs indicates many organizations may be underestimating the effort required to effectively execute the 2013 COSO framework.

[1] See minutes of the September 25, 2013, meeting of the Center for Audit Quality SEC Regulations Committee with the staff of the SEC. http://www.thecaq.org/docs/reports-and-publications/2013septembe25jointmeetinghls.pdf

The following should be of interest to finance and risk executives in banking and capital markets firms charged with guiding their organizations through this new internal control landscape.

1. Application of 2013 COSO framework

The 2013 COSO framework retains the three distinct, but overlapping categories of objectives – operations, reporting, and compliance – and reiterates the opportunity to expand the framework's application beyond its traditional adoption for external financial reporting to include operations and compliance.

While most banking and capital markets firms have used the COSO internal controls framework to design their SOX 404 compliance system of internal controls over financial reporting, many are now taking a broader view of the updated framework for other purposes. Current standards require the use of an accepted controls framework as the basis for complying with SOX 404; although, there is often no explicit mandate for the use of a formal framework for other regulatory, operational, and compliance activities.

However, the scrutiny of regulators and other third parties has intensified the need for the reporting to be the end-product of a well-controlled process, one in which the effectiveness of controls is periodically assessed. To that end, many banking and capital markets firms are using the principles of the COSO framework and have begun applying them to design quality assurance review functions over other areas, including operational and regulatory reporting.

2. Consideration of existing enterprise-wide controls programs

The 2013 COSO framework reemphasizes the control environment as the basis for carrying out internal control responsibilities across the organization. The framework also stresses the role of the board and senior management in setting the tone regarding the importance of internal control and expectations concerning standards of conduct (principles 1-5).

Many large banking and capital markets firms likely have several existing governance programs, processes, and monitoring activities that may help comply with the 2013 COSO framework. Examples include operational risk and control self-assessments, existing programs and communications to employees around ethics, values and expectations of conduct, and governance and oversight programs for outside service providers (OSPs). However, in many cases these processes may not have previously been considered part of the core SOX 404 program, and therefore, have not been formally evaluated as part of management's assessment of the effectiveness of internal controls over financial reporting. Consequently, as part of the efforts in 2014 to assess the gaps to comply with the 2013 COSO framework, management should consider creating an inventory of these existing risk governance programs, processes, and monitoring activities, as well as understanding and designing formal assessments as part of the SOX 404 program to demonstrate that they are present and functioning.

3. Dynamic risk assessment process

The 2013 COSO framework calls for companies to have a dynamic risk assessment program (principles 6-9) that considers significant changes in business operations and adapts to internal, external, and emerging risks.

To achieve such a dynamic risk assessment process, input from business units and appropriate levels of management should be formally captured as part of the risk assessment and scoping process, including the initial and continuous assessment of:

- Fraud risk
- Complex non-routine processes
- Processes requiring the "hand-off" of data between departments
- Manual processes or those dependent on end-user computing tools
- Potential changes in the internal control environment
- Emerging risks and issues at peer organizations and the industry

Further, the risk assessment should be periodically updated to capture changes, both internal and external to the company, which may impact the qualitative assessment of risks and corresponding selection of in-scope entities and controls, including general information technology controls, to be assessed as part of the evaluation process (principles 10-12). For example, some banking and capital markets firms have instituted periodic coordination processes throughout the year between the risk teams embedded in business lines and functions and the financial reporting risk and controls groups (i.e., SOX groups) to discuss changes in risk profile, emerging trends, and the external environment. These discussions are formally captured and revisions to the SOX program are assessed accordingly.

4. Outside service providers

The nature and extent of the use of OSPs today as compared to when the original COSO framework was written is exponentially greater and different. Because of the reliance that banks and capital markets firms place on OSPs, it is critical to have controls to monitor that OSPs are performing the expected role in the expected manner. Thus, it should be no surprise that the 2013 COSO framework incorporates concepts related to the use of OSPs in 12 of the 17 principles and emphasizes the inclusion of risks related to transactions processed by OSPs within the entity's risk assessment.

For many large banking and capital markets firms, having a robust vendor management program is essential to establishing and upholding a tenor of integrity and responsible action at OSPs. Such a program may include the OSPs within the banking and capital markets firms' ethics and integrity programs – extending the "tone at the top" beyond the walls of the organization. For example, several banking and capital markets firms include requirements for OSP employees to certify their understanding and compliance with the firms' standards of business conduct. Further, many formal vendor management programs also include provisions for OSPs to be monitored for compliance with contractual obligations and subjected to onsite review or audit of their operations. For banking and capital markets firms, the review and assessment of controls at OSPs may be critical to understanding the effectiveness of the OSPs' control environment. Banking and capital markets firms may need to review the robustness of their controls processes to ensure the appropriate level of control assurance as related to the OSPs that impact their financial reporting.

5. Fraud risk factors and fraud risk assessment

The 2013 COSO framework has been updated to specifically include concepts related to fraud risk (principle 8). Under the 2013 COSO framework, an organization should consider the various types of fraud (e.g., misappropriation of funds, fraudulent financial reporting, etc.) as part of its fraud risk assessment. Further, the assessment should include consideration of fraud risk factors, including incentives and pressure, opportunities, attitude, and rationalization.

While it is expected that most large banking and capital markets firms will have fraud risk programs specific to individual lines of business, a reassessment of fraud risks and their potential impact on a material misstatement of the financial statements may be required. Such a reassessment could lead to changes in controls that are considered relevant to external financial reporting.

In addition, a fraud risk assessment is generally not extended to OSPs and customers to capture external complaints and allegations. Several banking and capital markets firms extend code-of-conduct requirements, including anonymous disclosure of impropriety, to OSPs and vendors who are obligated to acknowledge such requirements annually (and that are similar to acknowledgements that internal employees must make). Allegations and results of investigations should be reported to those responsible for assessing the system of internal controls over external financial reporting.

6. Information to carry out internal control responsibilities

Recognizing the evolution of information systems and the increased dependency on system-generated information on the performance of internal controls, the 2013 COSO framework includes information technology considerations in 14 out of 17 principles. This includes consideration that information produced by the organization is complete, accurate, current, and verifiable.

In cases where the effective operation of internal controls requires information to cross departments, functions, or OSPs, as it often does, for example, to support fair value, derivatives, or commitment and guarantees disclosures, there is a risk that suppliers and users of the information may not fully understand how their information is being used and how the information is created. Understanding the upstream and downstream implications of data is critical to achieving an effective internal control environment.

Many financial statement disclosures require significant involvement and input from the business, product control, valuation, tax, and finance departments. To support the complete flow of transactions and ensure that all suppliers and users of information understand the requirements, banking and capital markets firms should:

- Inventory complex processes
- Document the end-to-end process and expected flow of information
- Identify the relevant controls that address the quality of the information generated and used in the performance of key controls supporting the financial statement line item or footnote disclosure
- Clarify roles and responsibilities that clearly articulate and confirm internal control objectives

Transition planning

While many banking and capital markets firms have recognized the need to perform an assessment comparing their current program to the 2013 COSO framework, consideration should be given to allow adequate time to respond to any potential gaps and enhancements identified and to implement the necessary changes to the existing internal control environment. The process to evaluate compliance with the 2013 COSO framework will require effort beyond a mapping exercise of existing programs, processes, and controls to the 17 principles associated with the five components of internal control. Banking and capital markets firms should anticipate the need for a potential increase in compliance effort, including assessing existing enterprise-wide control programs, putting in place a dynamic risk assessment process including a fraud risk assessment, evaluating the accuracy and completeness of information that is the basis for the system of internal control, and extending the internal control environment to OSPs. Management should commence its readiness assessments with urgency and expect significant discussion with its audit committee with periodic communication on progress throughout the year.

The 2013 COSO framework, while built on the same foundation as the previous version, is a reflection of an evolving business landscape – one in which the concepts of strong governance, adherence to risk principles, and the ubiquitous nature of information technology are key considerations for optimizing a risk management and internal controls structure. Risk management and internal controls have always been front and center in the banking and capital markets industry – and even more so now due to the constantly intensifying regulatory environment.

Heightened standards for the design and implementation of risk frameworks require a focus on governance, policies and procedures, risk monitoring and reporting, and internal controls, all of which are consistent with the 2013 COSO framework that can be applied across the organization.

We trust that these observations will assist in setting the context for leaders as they embark on the journey to comply with the 2013 framework.

To learn more, please contact:

Salvatore Davide
Partner
Deloitte & Touche LLP
+1 212 436 5459
sdavide@deloitte.com

Sandy Herrygers
Partner
Deloitte & Touche LLP
+1 313 396 3475
sherrygers@deloitte.com

Nitish Idnani
Principal
Deloitte & Touche LLP
+1 212 436 2894
nidnani@deloitte.com

Carol Larson
Partner
Deloitte & Touche LLP
+1 412 330 7210
clarson@deloitte.com

Todd Scarpino
Director
Deloitte & Touche LLP
+1 212 436 6276
tscarpino@deloitte.com