FinancialReporting

Deloitte.

Oduware Uwadiae

COSO – Takeaway for Banking and other financial institutions

Since 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, it is highly encouraged that the entity should begin moving forward with urgency towards its application

From our last articles on this subject, we have been able to establish that the COSO framework presumes that 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.

Since 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, it is highly encouraged that the entity should begin moving forward with urgency towards its application.

The following should be of interest to finance and risk executives in banking and other financial institutions charged with guiding their organizations through this new internal control landscape:

1. Application of 2013 COSO framework

The COSO framework has 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. Because of the scrutiny of regulators and other third parties, there is an intensified 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 organizations are encouraged to use the principles of the COSO framework and should begin 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 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).

Banks and other financial institutions in general likely have several existing governance programs, processes, and monitoring activities that may help comply with the 2013 COSO framework.

3. Dynamic risk assessment process

The 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).

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 not just banks, but many other 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 a large banking organization, 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 bank's ethics and integrity programs – extending the "tone at the top" beyond the walls of the organization. For example, a bank may include requirements for OSP employees to certify their understanding and compliance with the firms' standards of business conduct. Further, a formal vendor management program may also include provisions for OSPs to be monitored for compliance with contractual obligations and subjected to onsite review or audit of their operations.

5. Fraud risk factors and fraud risk assessment

The 2013 COSO framework specifically addresses 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. Nowadays, many organizations extend code-of-conduct requirements, including anonymous disclosure of impropriety, to OSPs and vendors who are obligated to acknowledge such requirements annually (and these are similar to the 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

Many financial statement disclosures require significant involvement and input from the business, product control, valuation, tax, and finance departments.

For a large banking organization, 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 bank's ethics and integrity programs – extending the "tone at the top" beyond the walls of the organization. For example, a bank may include requirements for OSP employees to certify their understanding and compliance with the firms' standards of business conduct

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:

- Make an extensive list of 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; and
- Clarify roles and responsibilities that clearly articulate and confirm internal control objectives

Oduware is the partner-in-charge of Accounting and Financial Advisory in Akintola Williams Deloitte