Deloitte.

Fraud risk assessments and COSO's 2013 internal control framework: Opportunities and common pitfalls

Although a majority of public companies have adopted the 2013 Internal Control – Integrated Framework ("the Framework"), published by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"), approximately one in four have remained with the original 1992 framework or have not disclosed which framework they have followed.[1]

Companies that have not yet adopted the Framework should take note of the following Securities and Exchange Commission (SEC) statement: "The longer [corporate] issuers continue to use the 1992 framework, the more likely they are to receive questions from the [SEC] staff about whether the issuer's use of the 1992 framework satisfies the SEC's requirement to use a suitable, recognized framework."[2] One area of focus in particular has been implementation of Principle 8, which explicitly requires consideration of the risk of fraud when assessing risks to the achievement of an organization's objectives.

In light of the new guidance and increasing scrutiny by the SEC, companies may need to revisit their current fraud risk assessment framework and implement new or enhanced procedures and considerations when assessing the risk of fraud. This article offers some insights into the implementation of fraud risk assessments ("FRA" or "FRAs") with emphasis on leading practice considerations and some common pitfalls.

The purpose and structure of FRAs

FRAs enable management of companies to identify the "who, what, where, and how" potential fraud schemes that may impact their organization. FRAs can assist management in identifying potential gaps in their internal control framework that could indicate an increased likelihood of fraud. Often, the basis for a FRA is a series of fraud brainstorm workshops with management from across the enterprise, aimed at identifying fraud risk factors, such as an increased pressure to meet earning targets; but also including the identification of specific potential fraud schemes without considering how likely or material the scheme would be.

Following the workshops and the development of a register of potential fraud schemes, consideration is given to the likelihood and potential impact of each fraud scheme in order to assess the inherent risk of each scenario. In addition, the organization's existing internal controls framework is considered to calculate a residual risk score for each scenario.

[1] "Report: Majority Adopt New COSO Framework," Tammy Whitehouse, Compliance Week, April 13, 2015, https://www.complianceweek.com/blogs/accounting-auditing-update/report-majority-adopt-new-coso-framework#.

[2] 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.

Opportunities and pitfalls associated with FRA implementation

Some organizations may underestimate the time, effort, and planning required to properly execute a FRA, particularly if the organization's first FRA is part of a 2013 COSO implementation. Being aware of the following leading practices when performing a FRA can help organizations effectively comply with the 2013 COSO requirements and avoid some common pitfalls:

Plan ahead and allow adequate time

Planning ahead in the process and allowing sufficient time to complete the FRA is the first step. Establishing a cross-functional working group to manage the FRA process can be helpful, along with assigning roles and responsibilities for the various components of the process. For example, the working group may include members of finance, internal audit, and certain business units, each with defined roles.

Involve relevant stakeholders

Considering that many of a company's internal controls relate to financial reporting, the finance department is a typical stakeholder in the FRA process. However, stakeholders from other functional areas, such as internal audit, information technology, human resources, compliance, legal, procurement, and business unit management, might also be included. Careful consideration should be given as part of the initial FRA planning to determine broadly where fraud risk may exist within the organization so relevant areas and business processes of the organization are included in the brainstorming discussions and subsequent FRA activities. Further, given the importance of the 2013 COSO framework and overall FRA process, it may also be prudent to include senior management as part of the process.

Disregard the control environment when identifying potential fraud schemes

Fraud can happen almost anywhere by or against an organization and be perpetrated by almost anyone, given the appropriate set of facts and circumstances. While an organization's internal controls may help mitigate the vast majority of potential fraud schemes, considering the controls during the brainstorming process may influence the brainstorm results themselves. Only when controls are set aside do stakeholders truly begin to put on the hat of a potential fraudster and identify potential fraud schemes that might be perpetrated within or against the company. After all, the fraudster may not be aware of fraud-prevention controls in place, or may work to circumvent controls.

Be specific when identifying potential fraud schemes

Organizations should try to identify not only where fraud might occur, but specifically how and by whom it may occur - for example, the individuals who would be involved, the access required of systems, the financial accounts impacted, and the electronic or paper trail which would be created, etc. The more specific the organization can be in the brainstorming process, the better able it is to assess and evaluate the potential likelihood and impact of a given fraud scheme.

Utilize a risk-based approach

Once fraud schemes have been identified, assessed and prioritized, it is important to spend additional time analyzing controls and processes, with the highest risk scenarios – those that if they were to occur, could have the greatest impact on the organization. Oftentimes, companies will spend a significant amount of time identifying controls for fraud schemes that while relevant, may not be of a huge impact to the organization, even if they were to occur time and again.

Don't forget to consider emerging risks

A FRA is not a "one-and-done" assessment. Organizations change, the macro-economy changes, and people change. There will always be new risks to an organization. For example, changes may result from new ways of conducting business, entering new markets, or bringing acquired businesses into the company culture. Recent technology advances may also present new risks not faced before by organizations. For example, the need to assess the risk of fraud in light of increased cyber attacks and a market that increasingly leverages shared technologies, such as cloud-based applications and data storage.

Document the FRA outcomes thoroughly

Organizations should look pragmatically at the results of the FRA to determine its overall conclusions about whether the organization's control environment and controls activities appropriately mitigate the potential fraud schemes identified. Insufficient documentation, including identification of risks at the scheme level, may make it more challenging for a company to demonstrate to regulators or auditors that they have adequately completed the requirements of the 2013 COSO framework.

A FRA is time well spent

A FRA is more than just another "box to check" in the changing regulatory landscape. A FRA carried out well can provide great insight into an organization's fraud risks and may lead to high-impact enhancements to the internal control framework. FRAs can lead to stronger controls and greater awareness that the company is monitoring fraud risks, and organizations should leverage the results of the FRA to potentially enhance monitoring activities carried out by internal audit, data analytics exercises, and the like.

The Association of Certified Fraud Examiners reports organizations on average lose five percent of revenue to fraud.[3] If an FRA results in increased awareness or internal controls that prevent just one fraud scheme from occurring, an organization may benefit from reduced fraud-related revenue and profit leakage, as well as less time and resources spent investigating and remediating fraud occurrences.

While the savings from conducting a FRA may not always be readily apparent or easily quantified, it may be simpler to compare the up-front investment of time and resources required to properly perform a FRA with the time and cost of suffering the effects of a fraud scheme which some individuals in the organization could probably have predicted might occur—if only someone had asked them.

[3]"Report to the Nations on Occupational Fraud and Abuse. 2014 Global Fraud Survey" Association of Certified Fraud Examiners. http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.

Contact

For more information, contact:

John Kim
Deloitte Advisory Director
Deloitte Financial Advisory Services LLP
+1 212 436 5342
jokim@deloitte.com

Holly Tucker
Deloitte Advisory Partner
Deloitte Financial Advisory Services LLP
+1 214 840 7432
htucker@deloitte.com