Deeper & Broader:
Performing Fraud & Reputation Risk Assessments

By Jonny Frank*

Internal auditors and other key players in the financial-reporting process are being pressured to step up their efforts to fight fraud. Legal, regulatory and standards-setting actions now require companies to develop effective antifraud programs, controls and risk-assessment processes, which independent auditors will audit annually. What's more, fraud and risks to reputation have become C-suite concerns, as reflected by a 2004 global CEO survey suggesting that more than a third of top executives worldwide view reputation risk – *which is viewed on a par with financial losses in many circles* – as a significant challenge[1].

As senior managements and audit committees strive to create stronger antifraud programs, they are increasingly asking internal audit to provide strong support to their corporate antifraud efforts. In response, best-practice internal audit departments cite the value of fraud risk assessments, which provide the cornerstones for many antifraud programs, acknowledging that an organization cannot control risks it has not identified.

Sooner or later, with antifraud efforts rising in importance, an internal audit department should expect to hear the following types of questions from management, the audit committee, or the independent auditor:

- What are the company's fraud and reputation risks?
- What programs and controls have been implemented to mitigate these risks?
- What is internal audit doing to prevent and detect issues before they emerge into a corporate scandal?

At public companies, such questions are likely to come *sooner* rather than later, so a proactive internal audit function will anticipate such queries and develop appropriate responses. In terms of risk mitigation, for example, the ability to perform thorough fraud and reputation risk assessments should be at the heart of any comprehensive antifraud program.[2] Assessments focusing on fraud and reputation risk are also an effective means

---

* Jonny Frank is a partner PricewaterhouseCoopers LLP, where he leads the Fraud Risks & Controls practice. He also serves on the faculty of the Yale School of Management, Fordham University Law School and Brooklyn Law School. The views expressed in this article are his own, and do not represent that of PricewaterhouseCoopers LLP, or the universities with which he is associated.

[1] 7th Annual Global CEO Survey, 2004, PricewaterhouseCoopers. Of 1,400 CEOs surveyed, 35% identified reputation risk as either "one of the biggest threats" (10%) or a "significant threat" (25%) to their business growth prospects.

[2] Key Elements of Antifraud Programs and Controls, a white paper published by PricewaterhouseCoopers in December 2003; is available at http://www.pwc.com.

to address SEC rules requiring controls related to the *prevention*, *identification* and *detection* of fraud[3]. In addition, such assessments are an essential first step in alleviating C-suite concerns about fraud and reputation risk.

Risk Assessments: How They Differ

All assessments are not alike. Fraud and reputation risk assessments build upon, but differ from, traditional risk assessments and those linked to Sarbanes-Oxley compliance. Traditional risk assessments link risks to an organization's key business objectives whereas Sarbanes-based risk assessments focus on financial reporting. As such, the Sarbanes-based risk assessment process thus begins with the significant accounts, disclosures and related assertions of the financial statements. The assessment targets the risk of material misstatement and evaluates implemented controls to prevent or detect material misstatements.

In particular, fraud and reputation risk assessments concentrate on fraud ***schemes*** and ***scenarios***. As such, the purpose of the risk assessment process is to identify various scenarios and schemes that can (a) significantly impact the organization's reputation, (b) expose the company to criminal or civil liability, or (c) result in a financial loss. The assessment team thus must be able to identify all the potential schemes and scenarios impacting the industries and geographic markets in which the organization conducts business.

In addition, assessments of fraud and reputation risk also focus on existing antifraud controls. The assessments need to examine whether controls can be circumvented as well as consider the susceptibility of controls to management override.

Gaining Management and Audit Committee Sponsorship

In many circles, fraud is the proverbial hot potato – too blistering to handle. For internal audit, that can be a plus, for senior management and the audit committee are likely to toss much of the operational responsibility for fraud management to internal audit while retaining ultimate authority and responsibility for antifraud efforts, as required by statutes, regulations and professional rules.

To be effective, fraud risk assessments require the strong endorsement of senior management or the audit committee. Without such backing, it would be difficult to unearth critical information about the organization's fraud risks residing with individual business units and business processes. In many instances, it is middle management and mid-level employees running day-to-day businesses who know where potential risks and skeletons lie.

[3] [3]See Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Securities and Exchange Commission Release No. 33-8238 (June 5, 2003) [68 FR 36636]

Obviously, unlocking such information can be tricky, due to fraud-related sensitivities and natural reluctance to talk about the subject. Employees and executives alike can be hesitant to furnish information because they fear suspicion, want to avoid the corporate spotlight, or are harboring someone's misconduct (their own, perhaps). As a result, internal audit can be hard-pressed to overcome this hesitancy without the active support of senior management or the audit committee.

In today's highly scrutinized business environment, internal audit ordinarily should expect to gain the support it needs from management and the audit committee. Often, all such support requires is raising the issue and offering the solution.

If you run into resistance, however, try these techniques:

- **Establish a Dialogue** – Fraud, albeit sensitive, is an interesting subject for discussion. Internal audit can quickly engender interest by engaging in one-on-one discussions with your general counsel, director of compliance, or the heads of business units and processes.

  To reach a larger audience on antifraud issues, internal audit can publish a **newsletter** periodically or establish a **centre of excellence** focusing on fraud. Such vehicles can bring fraud and misconduct closer to home. For example, publishing information about fraud and misconduct occurring within your same industry or geography will naturally lead company officials to question the vulnerability of your company to similar conduct

- **Leverage Sarbanes-Oxley §404 Readiness Projects**

  A company that does not conduct a comprehensive fraud risk assessment likely will receive a "significant deficiency" or "material weakness" from its independent auditor. Thus it's important for internal auditors of public companies to coordinate their fraud risk assessments with the organization's Sarbanes-Oxley readiness effort. At large multinational organizations, in particular, such coordination will also help simplify the assessment process, for Sarbanes-readiness projects identify the company's significant business units, processes, and locations. Internal audit can leverage this information to frame the scope of their fraud risk assessments. In addition, Sarbanes-readiness projects also inventory the organization's existing control activities, providing a resource for internal audit to draw upon in linking fraud risks to controls.

- **Host a Fraud Summit** – Although the C-suite and audit committee are concerned about fraud and reputation risk, they rarely discuss these subjects in an organized manner. At a dedicated fraud summit, internal audit can serve in a facilitating role to bring internal stakeholders together to discuss the areas of potential risk.

The ultimate goal, irrespective of vehicles, is for internal audit to engage senior management and the audit committee in the antifraud effort and persuade its overseers to take strong ownership of the antifraud program. The fraud risk assessment process will flow more smoothly if the organization understands that senior management and the audit committee are active sponsors of the activity.

Once senior management and the audit committee have given their active support to the corporate antifraud effort, you are ready to launch the risk assessment process.

The 7-Step Fraud Risk Assessment Process

Step 1: Organize the Assessment

Internal audit can integrate the fraud and reputation risk assessment process around the organization's existing business cycles or establish a separate cycle for this purpose. Organizing around an existing business cycle can simplify the process, for if internal audit is evaluating the revenue cycle, for example, the project team can expand the scope of the cycle to *specifically* consider fraud and reputation risks associated with revenue.

The downside to this approach is that internal audit may miss a fraud or reputation risk that does not fit neatly into a particular business cycle.

An alternative is to create a separate cycle focused on fraud and reputation risk. In doing so, however, consider a more innocuous title for the cycle, such as "safeguarding of assets," because of the anxiety-producing nature of a fraud descriptor.

Step 2: Determine Units & Locations to Assess

To be effective, fraud and reputation risk assessments must be conducted at the company-wide, business-unit and significant-account levels. Risk assessments should also be conducted when special circumstances arise, such as changed operating environments, the introduction of new products, the entry of new markets, and corporate restructurings.

At public companies, internal audit should liaise with the Sarbanes-Oxley readiness team because of its ongoing work with the organization's significant business units, accounts and locations. However, the fraud risk assessment process may well require a broader reach, given that reputation risk is not synonymous with financial significance.

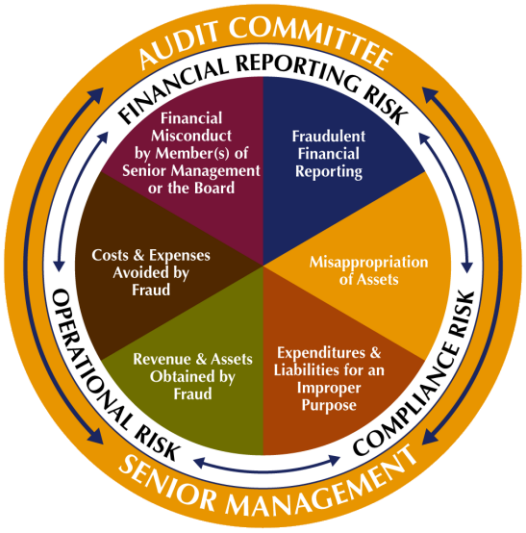
Multinational companies, for example, often conduct business at higher-risk locations. While such locations may not be financially material to the organization as a whole, there may be potential fraud and reputation risks associated with doing business in such markets, and both senior management and the board need to be apprised of such risks.

Step 3: Identify Potential Fraud & Misconduct Schemes & Scenarios

Organizations can damage their reputations or be defrauded in myriad ways. A critical step in the risk assessment process is to identify the organization's universe of potential risks – without regard to probability of occurrence (that consideration follows). Your starting point is to determine what fraud schemes and scenarios typically affect your

organization's industries and locations. Next, you must tailor these schemes and scenarios to your organization.

The challenge of developing a scheme- and scenario-based database for a company is formidable. PricewaterhouseCoopers has identified more than 150 generic fraud schemes, which fall into six basic categories: (1) fraudulent financial reporting[4], (2) misappropriation of assets[5], (3) expenditures and liabilities for an improper purpose[6], (4) revenue and assets obtained by fraud[7], (5) costs and expenses avoided by fraud[8], and (6) financial misconduct by senior management[9]. The risk assessment process must address all six categories of fraud and misconduct to avoid a "significant deficiency".



These schemes differ drastically by product and service sector and geography. However, these 150 generic fraud schemes are just the tip of the iceberg. For example, sales and marketing schemes are quite common in the Asian market whereas procurement fraud is more widespread in Central and South America. On the other hand, the types of schemes affecting a bank will differ from those affecting a manufacturer. While both companies may be obtaining assets in a fraudulent manner, the bank might do so by failing to credit

[4] Most fraudulent financial reporting schemes involve earnings management, arising from improper revenue recognition, overstatement of assets or understatement of liabilities. Fraudulent financial reporting can occur at the entity or business-unit level.

[5] Misappropriation of assets involves external and internal schemes, e.g. embezzlement, payroll fraud, and physical theft, as well as hard (inventory) and soft (intellectual property) assets.

[6] This category refers to commercial and public bribery as well as other improper payment schemes.

[7] This category refers to those fraud schemes where the organization commits a fraud against its employees and/or third parties.

[8] Tax fraud is an example where an entity avoids an expense through fraud.

[9] Financial misconduct by senior management is considered a separate category because of the serious legal, financial, and reputation risks that can arise. Indeed, the proposed PCAOB auditing standards mandate a finding of a significant deficiency in controls if fraud on the part of the senior management of "any magnitude" is identified. PCAOB ¶126.

interest or by charging improper fees whereas the manufacturer may be short-shipping a distributor to obtain assets fraudulently.

The typical large multinational company, as a result, faces hundreds, if not thousands, of fraud and reputation risks. To develop scheme descriptions for your organization requires a deep knowledge of fraud, the industry or industries in which your organization operates, and the geographies where you conduct business.

In all likelihood, your organization will look to internal audit to provide the requisite fraud expertise. In turn, internal audit will need to know (1) the technicalities and mechanics of each scheme and sub-scheme, (2) scheme indicia, (3) antifraud preventive & detective control activities, and (4) fraud-auditing procedures. You will also need to keep track of new and emerging frauds in your organization's industry and geographies.[10]

Internal audit can draw relevant information from individual business units about industries and geographies served. Note, however, that it is one thing to be an industry and geographic expert – but quite another to be expert about how fraud and misconduct occur and can be mitigated. Your country manager, for example, is a critical starting point, but it's essential to cover all bases. Publicly available information about fraud schemes tends to be quite limited and generic in nature, reflecting both the reticence of companies to share information about such matters as well as the scant attention given to fraud prevention and detection prior to the early 21st century corporate scandals.

Your organization's assessment team also needs to understand the risks and ramifications posed by each scheme. The risks generally include: (1) reputation risk, (2) financial risk, and (3) legal risk. Senior management and the audit committee will likely be more willing to accept the financial risk of losing money to fraud than they will the loss of reputation or the possibility of criminal or civil sanctions.

Step 4: Assess Likelihood of Fraud

Fraud risk assessments, like traditional risk assessments, consider the likelihood that a particular fraud will occur. The proposed PCAOB auditing standards would modify traditional auditing levels[11] to specify the following risk levels:

- Remote
- More Than Remote
- Reasonably Possible
- Probable

[10] PricewaterhouseCoopers maintains a database of newly reported frauds. Our sources include the media, reporting services, and industry associations and experts.

[11] The proposed PCAOB standards refer to Financial Accounting Standards Board Statement No. 5, *Accounting for Contingencies* (FAS No. 5), which uses the terms probable, reasonably possible and remote. The proposed PCAOB standard adds "more than remote" as an additional level.

Under the proposed standards, an organization must address risks that have "more than a remote" likelihood of occurring to avoid a significant deficiency. Fraud risks deemed to be remote can be ignored, although it is advisable for the assessment team to document that the organization had considered the risk before determining it to be remote.

Step 5: Assess Significance of Risk

Next, assess the significance of fraud risks with a more than remote likelihood of occurring. In this context, the proposed PCAOB standards refer to:

- Inconsequential
- More Than Inconsequential
- Material

The term materiality refers to the significance of an item to the users of a set of financial statements.[12] SEC registrants should note that SEC Staff Accounting Bulletin (SAB) 99, which provides guidance in determining materiality when fraud is discovered[13], rejects the frequently used rule of thumb that a misstatement or omission that is less than 5% of some factor (e.g., net income or net assets) is immaterial. SAB 99 requires that a determination of materiality consider both the "quantitative" and "qualitative" aspects of the particular matter being analyzed. Fraud rises to the level of materiality if a reasonable person – say a shareholder or lender – would consider it important.

When evaluating significance, internal audit should consider the impact of the fraud scheme individually and in the aggregate. Some frauds, such as travel and expense fraud, might be inconsequential on an individual basis but be significant on a combined basis.

Organizations must address fraud risks that are "more than inconsequential" in amount to avoid a significant deficiency. Although the organization can ignore fraud risks deemed to be inconsequential, based on cost-benefit considerations, it should document why this determination was reached.

Step 6: Link Antifraud Controls

Next, internal audit should identify the control activities for those fraud and reputation risks that have a more than remote likelihood of occurring and that are more than inconsequential in amount. Proper assessments of fraud and reputation risk specifically demand that internal audit consider whether and how the controls can be circumvented or overridden by management and others.

---

[12] Financial Accounting Standards Board ("FASB") Statement of Financial Accounting Concepts No. 2, Qualitative Characteristics of Accounting Information ("FCON 2") describes materiality as "[t]he omission or misstatement of an item in a financial report is material if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item."

[13] 17 Code of Federal Regulations Part 211, August 12, 1999.

Furthermore, internal audit should identify fraud risks which cannot be tied to effectively designed and operating controls. Where control weaknesses result in more than a remote likelihood of fraud loss at more than an inconsequential amount, corrective measures should be considered. Ultimately, management and the board will need to conduct their own cost-benefit analysis of the costs of controlling a risk vs. the benefits of mitigating or eliminating that risk. However, should management decide against implementing corrective measures, it's important to document their analysis.

As a rule of thumb, antifraud controls generally include controls designed to *prevent* fraud and those designed to *detect* fraud *in a timely fashion* when it occurs. Internal audit should expect to tie 70% to 80% of identified fraud risks to existing control activities such as approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets.

Step 7: Demonstrate Impact on Audit Plan

Finally, internal audit should consider (and document) the results of the fraud and reputation risk assessment in developing its audit plan. Fraud auditing likely will be required to address residual fraud risks, i.e., fraud risks that are not mitigated by preventive or detective control activities.

Ready, Set, Go …

Once the fraud and reputation risk assessment has taken place, internal audit will need to evaluate and test the design and operating effectiveness of antifraud controls. The process for evaluating antifraud controls is similar to testing other control activities. Coordinate with your independent auditor, since the proposed PCAOB standards require an independent evaluation of antifraud controls, that is, the independent auditor cannot rely upon internal audit's testing of antifraud control activities. Some organizations will opt to leave the testing to the independent auditor whereas others will want to conduct their own testing in advance.

Fraud auditing is a new field that combines aspects of forensic investigation and standard auditing techniques. Fraud auditing relies upon standard auditing techniques – such as interviews, analytics and substantive procedures – that have been modified to detect indicia of a fraud scheme. In addition, fraud audits typically require knowledge of how frauds can occur in various industries as well as a firm grounding in the *indicia* for the fraud schemes being audited. However, fraud audits differ significantly from forensic investigation, although both fraud auditors and forensic investigators must have fraud training. While an investigation is an inquiry into specific allegations or suspicions of fraud, a fraud audit is a search for indicia of fraud.

In conducting fraud auditing, don't overlook computer-assisted auditing techniques (CAATs) to search for indicia of fraudulent activity. CAATs, because of their ability to search massive amounts of data, can be quite helpful when searching for the proverbial needle in a haystack.

Some Closing Thoughts

A fraud and reputation risk assessment is the corporate equivalent of a visit to the dentist: Senior management and the board expect pain, yet anticipate relief if the assessment determines that the organization's fraud and reputation risks are under control.

By reducing fraud, a company can trim costs and improve profitability, and to the extent that internal audit can help reduce fraud, it will contribute mightily to the organization.

Antifraud controls are required by law, and fraud risk assessments are the cornerstones of an effective antifraud effort. They provide an excellent means for internal audit to provide significant organizational value and gain a higher profile with the audit committee and senior management.

And of particular note, antifraud efforts have the potential to more than pay for themselves. A major study of the insurance industry demonstrated that for every dollar invested in antifraud programs, the return on investment was nearly $7[14]. Likewise, benchmarking analysis and research by the General Counsel Roundtable found that each additional dollar of compliance spending saves organizations, on average, $5.21 in heightened avoidance of legal liabilities, harm to the organization's reputation and lost productivity. That's more than a five-to-one payback per dollar of compliance investment[15].

What better way to add organizational value.

[14] **"**Insurance Fraud: The Quiet Catastrophe**,"** Insurance Research & Publications, Conning & Co., 1996. The Conning study, which sought to project returns on investment for combating insurance fraud, defined ROI as the ratio of money saved to money spent preventing fraud. It found that the average ROI across the insurance industry for 1995 was $6.88 for every dollar spent on fighting fraud. (Source: Coalition Against Insurance Fraud)

[15] "Seizing the Opportunity, Part One: Benchmarking Compliance Programs", © 2003 Corporate Executive Board, General Counsel Roundtable.