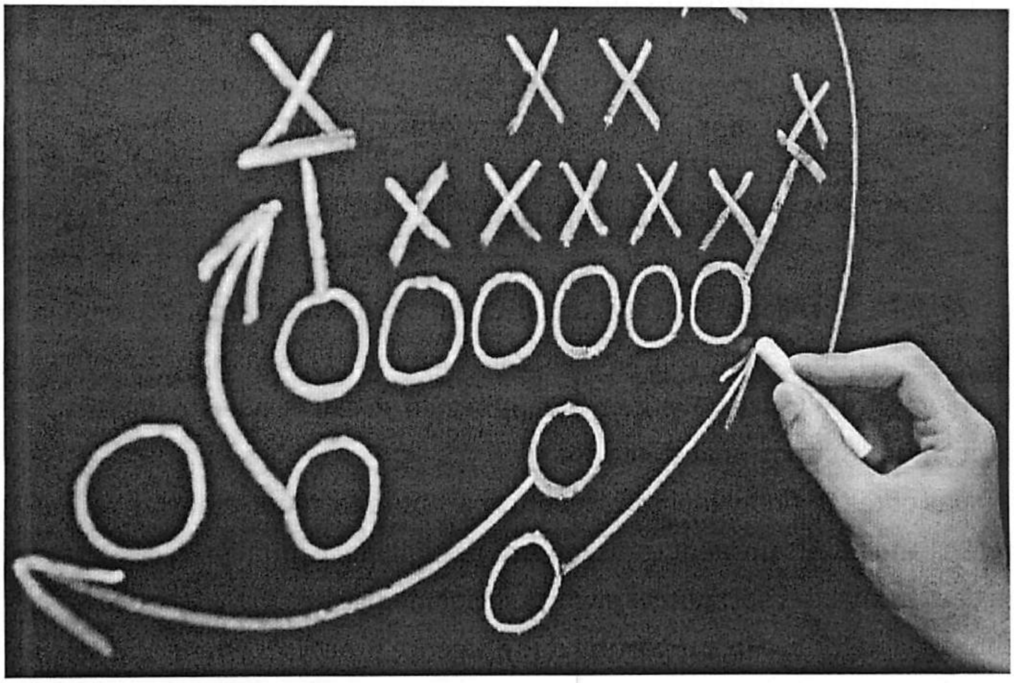
fei. | Daily

Become Proactive, Not Reactive, to Anti-Fraud and Anti-Corruption Programs

Carolyn J. Newman and Darryl S. Neier August 26, 2014 5:52 am

The U.S. Securities and Exchange Commission and the U.S. Department of Justice have stepped up their games in identifying and investigating possible accounting fraud and foreign corrupt practices.



© IVELIN RADKOV/ISTOCK/THINKSTOCK

The consequences for companies who come under scrutiny by these federal agencies are costly in terms of time, distraction, possible fines and reputation. Legal professionals mostly agree that fines can be limited for those companies that demonstrate an effective compliance program is in place.

Trends in Fraud and Fraud Detection

The Association of Certified Fraud Examiners' 2014 Report to the Nations found that, while less than ten percent of the cases in the survey involved financial statement fraud, the median financial impact of those cases was $1,000,000. Tips are the most common form of detection (43%); however, the proactive methods for fraud detection – management review, internal audit, plus account reconciliation activities (combined) – detected 40% of financial statement frauds. Twenty-six percent of those cases were perpetrated by executive management and

17% were perpetrated by the sales department. Financial statement fraud cases appeared most frequently in three industries: construction, oil & gas and manufacturing.

Entitled "Overcoming Compliance Fatigue," EY's 2014 GlobalFraud Survey revealed that fraud risks are not declining, and noted "The willingness of respondents to justify certain activities when under financial pressure shows an interesting correlation with their role.

- CFOs are more likely than any other role to justify making changes to assumptions relating to valuations and reserves to meet financial targets.
- General counsel respondents are more likely than others to justify backdating contracts to meet financial targets.
- Sales and marketing respondents are most likely to justify introducing more flexible return policies to meet financial targets.

Based on its Global Forensic Data Analytics Survey, EY recommended companies consider expanding the use of forensic data analytics (FDA) as a means of enabling companies to maximize how their own information can be used to identify fraud indicators and support investigations.
The focus of testing may include accounts payable and vendor master data, expenses and entertainment transactions, payroll and capital projects data, and even data from external sources such as social media sites.FDA was also recommended for use in supporting due diligence processes when considering risks of bribery and corruption at targets for acquisition or third-party agency relationships.

PwC's 2014 Global Economic Crime Survey found notable increases from 2011 to 2014 in accounting fraud, bribery and corruption fraud and procurement fraud. Participants also reported less frequency for performing annual (or more often) fraud risk assessments. Major frauds were detected by suspicious transaction reporting/data analytics by 25% of participants in 2014, compared to 18% in 2011. The rise in use of data analytics was thought to be a reason for the increase in accounting and corruption frauds, since the proactive nature of these activities would uncover more instances.

The Importance of Fraud Risk Assessments

One of the most significant changes to COSO's updated Internal Controls Framework is the inclusion of Principle 8, incorporating the concept of assessing fraud risks. It specifically names these concepts related to considering risks associated with various types of fraud:

1. Fraudulent financial reporting
2. Misappropriation of assets
3. Corruption and other illegal acts
4. Management override of controls

It also discusses the need to assess the fraud risk triangle: incentives and pressures, opportunities, attitudes and rationalizations that could lead to fraud. Demonstrating compliance with Principal 8 involves entity-level fraud risk assessments where fraud risks are linked to relevant financial statement assertions.

Fraud risk assessments are designed to help identify fraudulent activities that could occur in an organization, then linking each fraud risk to the affected business process. Management can use the fraud risk assessment to determine courses of action when incidents of fraud are uncovered, then how to implement stronger controls that will prevent future fraud risks. These assessments need to be analytical in addition to reviewing the control environment and information technology structure.

Best practices would dictate that these assessments be conducted in phases:

Phase 1: A comprehensive review of the administrative, operational and financial systems of the company or organization. This phase includes individual interviews of key personnel, discussion with management, initial document review, and an initial assessment of the control environment and culture.
Phase 2: In this phase a forensic analytical review is conducted of vulnerability areas identified in phase 1 along with testing other financial areas. Computerized data interrogation/analysis software such as CaseWare IDEA is utilized to look for patterns in financial data in addition to non-traditional auditing techniques. The risks once identified are scored low to high.
Phase 3: Working with management the risks are reviewed and new procedures are developed for faster reporting of potential fraud and minimizing the company or organizations exposure.

Strengthening Anti-fraud and Anti-corruption Program

While public companies and those with international operations have regulatory concerns to help justify strong anti-fraud and anti-corruption programs, the main reason to focus on them and to demonstrate compliance is for the good of the organization. A culture of integrity creates confidence in the organization's ability to meet objectives. The written plan, code of conduct and standard operating procedures are nothing but form over substance if those policies are not well communicated (with training provided) and followed from the top of the organization to its line employees and third-party participants. Does everyone in the organization know what fraud schemes are most common in the industry and how to recognize them?

When a fraud or other act of noncompliance occurs, the final impact will depend on management's reaction and handling of the matter. Therefore, anti-fraud and anti-corruption programs must outline consequences and management must stick to them. Since the devil is always in the details, any program that does not include tools for proactively looking for exposures and opportunities for fraud to occur is incomplete. Two tools are most effective:

1. Proactive responses to tips (data analytics can be applied to the database of tips to identify patterns and further exposures)
2. Data analytics capabilities to continuously test for errors, anomalies and possible fraud

These tools are relatively inexpensive. They represent that ounce of prevention that's worth a pound of cure. How can tip lines and data analytics focused on detection become preventive controls?

- By reinforcing the stated goals for anti-fraud and anti-corruption programs
- By focusing on the results of tests and allowing for root cause analysis
- By shining a light on errors and anomalies that might become opportunities for future fraud
- And by monitoring in a way that documents the process and facilitates a continuing improvement to the controls and mitigation of fraud risks

Through effective analytics, you can answer questions that might help you head off potential fraud or corruption, or identify regulatory risks or even improve processes for more timely and accurate financial and operating information such as:

Who are my highest bonus or commissions earners and what might they be doing

to game the system?
Are travel and entertainment polices being followed and where are the potential risks of expense reimbursements abuse?
Are there abuses in my P-card program that are creating a culture of noncompliance?
What instances of lapses in segregation of duties might be occurring that are creating losses?
How can I ensure the quality of data and the accuracy of my transaction monitoring for AML?
How can I speed up the reconciliation process to find errors more quickly?

What Does This All Mean?

Technology has played a significant part in helping companies grow their systems and controls. Financial professionals and management should take advantage of data analytics using professional-level tools because it enhances the risk assessment process and provides the ability to "detect potential misconduct that we couldn't detect before" (89% according to EY's Global Forensic Data Analytics Survey 2014). The designed tests can then fuel automated monitoring capabilities to continually improve the detection of fraud with a goal of either preventing instances or minimizing their effects. It sends the message to all potential fraudsters: we're watching and we will take action on identified fraud. Effective anti-fraud and anti-corruption programs are a key part of a good internal controls system.

And that's good for businesses everywhere.

Carolyn J. Newman, CPA.CITP, CISA is president of Audimation Services, Inc. – the U.S. business partner of CaseWare Analytics. Darryl S. Neier, MS, CFE is the Principal in Charge of Sobel& Co., LLC Forensic Accounting and Litigation Services Group.