Deloitte.

Managing the business risk of fraud:
New guidance for a new risk environment

Centre for Corporate Governance

Many antifraud professionals believe that organizations today face a greater risk of fraud occurring than ever before. Current business trends, such as supply chain globalization and further reliance on information technology, coupled with economic instability, have increased both the pressures and the opportunities for fraud to occur. Additionally, organizations must respond to the heightened public and regulatory scrutiny, and the potential for reputational damage that follow fraud allegations. In this climate, organizations would be well-advised to take a fresh look at their fraud risk management practices.

New professional guidance, *Managing the Business Risk of Fraud: A Practical Guide*[1], provides timely and valuable information about how to design an effective fraud risk management program. This new guidance, issued by the Institute of Internal Auditors (IIA), the American Institute of Certified Public Accountants (AICPA), and the Association of Certified Fraud Examiners (ACFE), shares leading practices and recommended steps to improve fraud risk management processes.

This point of view paper from Deloitte summarizes the key messages in the guidance, and provides additional suggestions for executives facing the practical challenges of fraud risk management process design and implementation

[1]Managing the Business Risk of Fraud: A Practical Guide, published June 2008 by The Institute of Internal Auditors, the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners.

Why should my organization be especially concerned about fraud now?

Recent developments suggest that the level of fraud risk facing many organizations has increased.

1. Globalization

As many organizations expand around the world to source supplies from other countries, or to expand their sales in emerging markets, they may encounter complex risks for which they may not be prepared. These risks range from bribery and corruption, to compliance with export controls and anti-money laundering statutes, to product quality risks that can endanger customers. Enforcement by the Indian Agencies like Anti Corruption Bureaus, CBI in light of Indian Prevention of Corruption Act (IPCA), 1988, Prevention of Money Laundering Act, 2002 (PML Act) and by U.S. Department of Justice of the Foreign Corrupt Practices Act (FCPA) has also increased dramatically. All of these pressures are driving national, multi-national corporations to manage the global financial, regulatory, and reputational risks associated with fraud and corruption.

2.Economic downturn

The current slowdown in the economy can make it more difficult for executives and managers to achieve planned results. It is also putting more employees under personal financial pressure. Fraud specialists suggest that economic pressures increase the likelihood and the number of individuals resorting to fraud to achieve corporate objectives or to meet personal needs. Financial losses due to fraud are additional costs that organizations will have a hard time absorbing, especially at this point in the economic cycle.

Economic downturns put more pressure on executives and employees, thus increasing the likelihood of good people doing bad things, like committing fraud.

3. Risk management surprises

From the mortgage crisis to the "rogue trader" cases, recent events suggest that even organizations with risk management programs in place can be vulnerable to fraud. Some past assumptions about risk management and fraud risk assessments may now be obsolete. While technology has helped us run our businesses more efficiently and created new and better fraud monitoring capabilities, it has also added a level of complexity and exposure to fraud risk management.

Recognizing the importance of sound risk management policies, Standard and Poor's (S&P) recently announced that it would begin including an evaluation of enterprise risk management as a component of its independent credit ratings and credit analysis[2]. Deloitte's belief is that the mere existence of risk management programs and antifraud controls may give some companies a false sense of confidence. Now may be the time for organizations to re-evaluate their programs and determine whether they are sufficiently detailed to withstand new complexities, new fraud risks, and external scrutiny.

Many companies are still as vulnerable to fraud today as they were pre-Sarbanes-Oxley. Unfortunately, too many companies don't act to improve their fraud risk management program until they have a fraud event and the damage is already done.

[2]For more information on the S&P announcement, see http://www2. standardandpoors.com/spf/pdf/events/CRTconERM5908.pdf.

4.Room for improvement

Certain evidence suggests that current fraud risk management programs at many organizations need improvement. A survey by the Deloitte Forensic Center, *Ten Things About Fraud Control: How Executives View the 'Fraud Control Gap*[3]' revealed a substantial "*fraud control gap*" between organizations withmore effective antifraud programs in place and those operating with less effective antifraud measures[4]. Moreover, even the organizations considered more effective in detecting and preventing fraud demonstrated significant opportunities to enhance their performance.

Based on the survey results and our experience with antifraud programs and controls, Deloitte sees six key areas where most organizations can improve their fraud risk management programs:

- Fraud risk assessment
- Fraud control policy
- Monitoring of third-party relationships in the supply chain
- Employee fraud awareness training and surveys
- Hotline benchmarking
- Investigative response plan

[3]The Deloitte Forensic Center's study was conducted in the summer of 2007 and published in November 2007. *Ten Things About Fraud Control* can be downloaded at: www.deloitte.com/us/forensiccenter.
[4]Companies were categorized into those that were more effective at fraud control and those that were less effective. Companies were considered as more effective when executives gave their companies an average rating of 3.5 or greater (on a five-point scale) on their effectiveness in four areas: preventing internal fraud, detecting internal fraud, preventing external fraud, and detecting external fraud; less effective companies were those receiving average ratings of less than 3.5.

What are the benefits of fraud risk management?

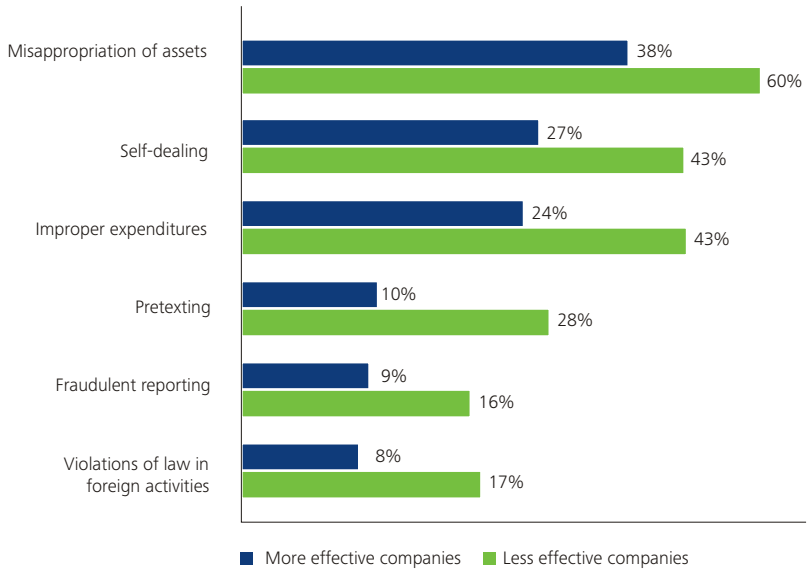
Strong fraud risk management makes good business sense. In our experience, organizations that implement detailed fraud risk management processes can also experience related benefits, including:

- Reduced financial losses due to fraud
- Reduced costs of responding to fraud (investigations, legal costs, and regulatory enforcements)
- Compliance with applicable Indian regulations, such as the IPCA,PML Act, Clause 49 of listing agreement & International regulatory,requirements such as Sarbanes-Oxley Act, SAS 99, AU316, AS5, FCPA, the U.S. Patriot Act, U.S. sentencing guidelines, J-SOX, C-SOX, and the Organization for Economic Co-operation and Development (OECD), among others
- Enhanced ethical culture ("tone at the top")
- Improved employee sensitization to and awareness of fraud
- Increased reporting of potential frauds and other ethical issues
- More effective corporate governance and the potential for improved governance ratings

Executives from organizations considered to be more effective at fraud control, surveyed for *Ten Things About Fraud Control,* anticipated that instances of fraud were much less likely to occur over the next 12 months as compared with organizations with less effective fraud controls. The perceived "fraud control gap" between more effective and less effective organizations is particularly striking in the areas of fraudulent reporting (such as "cooking the books") and violations of law in foreign activities (such as FCPA violations). These fraud risks can have serious financial and reputational consequences and are of great concern to most directors and officers surveyed.

Executives at more effective organizations anticipated that instances of fraud were much less likely to occur over the next 12 months

Percent of executives responding that fraud is somewhat likely, very likely or extremely likely



Real World Example

Prior to establishing a claims investigation group, a company annually paid out millions of dollars relating to insurance claims, many of which were false. After establishing an antifraud investigation group, the company saved millions of dollars annually in false claims, thus repaying the cost of the group many times over.

What lessons may be learned from the new guidance?

The new guidance, *Managing the Business Risk of Fraud: A Practical Guide*, provides executives with information about leading fraud risk management practices, and it shows how the different elements of a fraud risk management program can work together to create a more effective whole.

The guide can be used to help evaluate and strengthen an organization's existing fraud risk management program, or to assist in designing and implanting new processes. The principles and strategies outlined in the guide are not only for public companies, but also can be applied by private companies and smaller organizations, as well as nonprofits and governmental entities by making adjustments for different governance structures.

Five key elements of fraud risk management

The new guidance identifies five key elements of fraud risk management. We discuss each of these elements below.

Key Elements of Fraud Risk Management from "Managing the Business Risk of Fraud"

1. Fraud risk governance
2. Fraud risk assessment
3. Fraud prevention
4. Fraud detection
5. Fraud investigation and corrective action

What role does fraud risk governance play?

The new guidance emphasizes the need for an organization's board of directors or other governing body to ensure that its governance practices set the tone for fraud risk management. Management should implement policies that encourage ethical behavior. The roles and responsibilities for personnel at all levels of the organization involved in fraud risk management should be defined clearly.

In addition to the new guidance, Clause 49 of the Stock Exchange Listing Agreement addresses the oversight role that the board of directors, especially the audit committee, must perform with regard to risk management. The fraud risk management responsibility of those charged with governance is an important fiduciary duty that requires adequate time and resources to respond to the charge.

While many organizations have a process that governs fraud risks, common opportunities for improvement in this area include:

- Implementing effective board of directors oversight of fraud risk management
- Establishing a formal fraud control policy/strategy
- Creating a cross-departmental committee (e.g., internal audit, security, legal, human resources, supply chain, accounting, finance, etc.) to address fraud risk management and to periodically update the board and the audit committee
- Appointing an executive-level member of management responsible for leading the committee and coordinating fraud risk management efforts
- Formalizing roles and responsibilities of the board, audit committee, management and staff related to fraud risk management

There is something of an 'identity crisis' facing fraud risk management today. Too many organizations are operating under the misconception that antifraud programs are the responsibility of one designated function alone, such as internal audit, loss prevention, or security. Successful fraud risk management cannot occur without each department playing a role in preventing, detecting, and responding to fraud.

How important is fraud risk assessment?
Performing an effective fraud risk assessment is the cornerstone of a fraud risk management program. The new guidance recommends that a fraud risk assessment address relevant key areas and be tailored to the organization's size, complexity, industry, and goals. The organization should perform and update its risk assessment regularly to understand evolving fraud risks and the specific vulnerabilities that may apply to the organization over time.

A detailed fraud risk assessment should identify what types of fraud an organization is most susceptible to, where inside or outside the organization it could occur, and how it might be perpetrated. These identified fraud scheme risks should then be prioritized based on their significance and likelihood and subsequently linked to mitigating programs and controls. In our experience, this level of detail benefits the organization by fostering risk intelligence - an informed, balanced, and dynamic approach to risk management.

Opportunities for performance improvement in the area of fraud risk assessment typically include:
- Linking risks to specific control activities
- Involving personnel at all levels
- Focusing on the risk of management override of internal controls
- Conducting assessments for key business units and key countries
- Performing detailed assessments at the fraud scheme level

Real world example
Even though a company had been performing a fraud risk assessment in the past, it did not consider how
it was vulnerable to specific fraud schemes. After performing a detailed fraud risk assessment, the company identified exposure to collusive fraud in its treasury function that was unmitigated by any controls. As a result, the company instituted an additional control for treasury disbursements that identified a collusive cash defalcation scheme, which had been occurring and had gone undetected for some time. Making its fraud risk assessment more detailed by considering fraud schemes and mitigating controls helped this company to identify fraud and to minimize its financial losses.

Real world example
Fraud detection technology helped one company detect potential fraud, waste, and abuse by flagging common bank account numbers between employees and vendors. Further investigation of these flagged accounts indicated that an employee had diverted millions of dollars in legitimate vendor payments to his own bank account. The company was able to recover the monies and mitigate the access control that allowed the incidents to occur.

What are the keys to fraud prevention and detection?
While it is not possible to eliminate fraud entirely from an organization, the right prevention and detection measures can significantly mitigate fraud risks. This section of the new guidance emphasizes that fraud prevention is the first line of defense in reducing fraud risk. Organizations can increase their fraud prevention efforts through continuous communication and reinforcement. The guide also reminds us that "one of the strongest fraud deterrents is the awareness that effective detective controls are in place.[5]"

In our experience, common improvement opportunities in fraud prevention and detection include:
- Improving employee fraud awareness training
- Re-prioritizing fraud detection efforts onto key fraud risks
- Greater use of technology to enhance fraud detection and deterrence
- Benchmarking fraud helplines/hotlines to uncover performance issues

Executives charged with fraud risk management are often unsure where to start or are simply overwhelmed by the task ahead of them. One of the outcomes of a fraud risk assessment is a prioritization of fraud risks. Figuring out where you are and where you need to be is half the battle.

Too often, companies fail to put a fraud allegation investigative response plan in place and are caught off-guard at a time when prompt action is needed.

[5]Managing the Business Risk of Fraud, A Practical Guide, page 9

What are the leading practices in fraud investigation and corrective action?

Recognizing that no system of internal control can completely eliminate fraud, the guidance includes recommendations for conducting investigations and taking corrective actions. The guidance suggests that the board of directors take responsibility for seeing that the organization develops a system for prompt, competent, and confidential review and investigation of allegations involving potential fraud or misconduct.

The new guidance also shares leading practices for receiving, responding to, and evaluating allegations of fraud. Furthermore, it recommends specific tasks for conducting an investigation, including interviewing, evidence collection, computer forensic examinations, and evidence analysis.

We believe that most organizations could benefit from incorporating leading practices into their investigative response plans including:

- Establishing and documenting fraud investigation protocols
- Identifying fraud investigation resources, especially global response teams, in advance of a crisis
- Implementing a case management system to track and log the resolution of fraud allegations

Implementing processes and control improvements enterprise-wide to gain efficiencies and prevent recurrences

Real world example

For many years, a major international company performed audits of its employees' travel and expense claims without identifying any major frauds. However, after expanding its fraud awareness training to all overseas locations, the company received several alerts through its whistleblower hotline. The allegations related to misuse of authority and override of controls by senior executives at an overseas location that was never subject to a full scale internal audit due to its small size. The resulting investigation revealed corruption and serious violations of the code of conduct by senior executives at this location. Better awareness of fraud risks and an appreciation for headquarters' commitment to ethics influenced the whistleblowers to report such activities.

How can my organization use the new guidance?

The most important message to take away from *Managing the Business Risk of Fraud* is that fraud risk management is dynamic. As businesses change and grow, so do their fraud risks. We recommend a continuous improvement approach to fraud risk management that requires regular measurements of where

the business is and where it wants to be in terms of effectively deterring, detecting, and preventing fraud. We call this approach the Measure, Improve, and Move methodology.

Measure, improve and move

Evaluate	Identify Risk	Action Plan	Mitigate	Monitor	Respond
Analyze the current status and effectiveness of the approach to implementing antifraud programs and controls within the business	Assess, define, and document fraud risks and control effectiveness; establish fraud risk profile by analysis of risk against controls	Help prepare an action plan to address areas of fraud risk identified for control improvement or new control implementation during the fraud risk assessment	Enhance, implement, and maintain preventative and detective control activities which help mitigate fraud risks identified during the fraud risk assessment	Help enable continuous monitoring activities through and ongoing review activities to alert management of potential fraud; incorporate findings into annual fraud risk assessment process	Assist in responding to potential occurrences of fraud within the Business

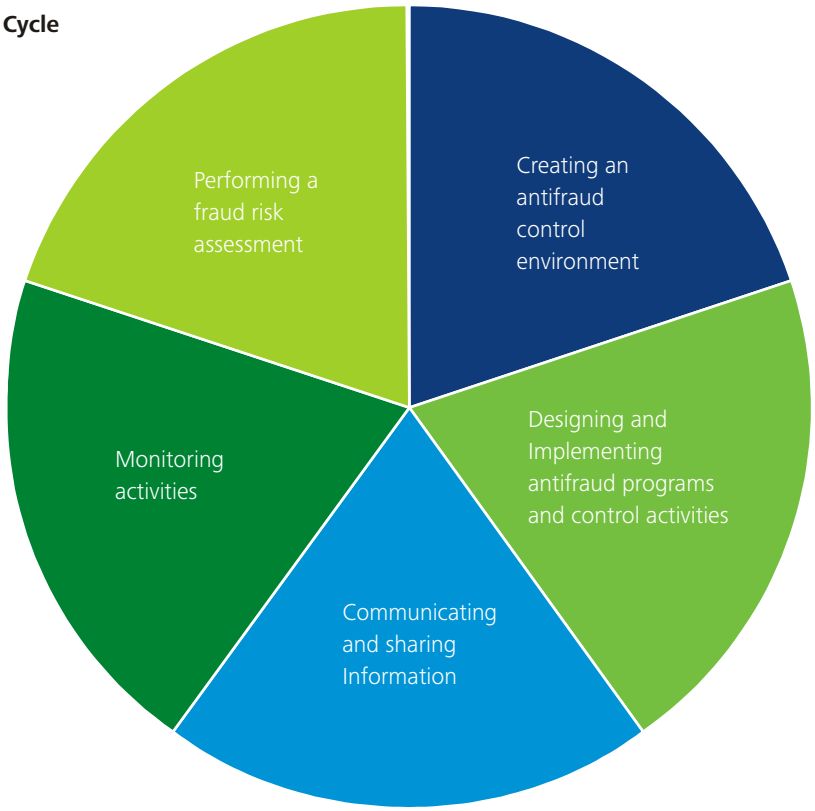
Responding to the new guidance

- **Make fraud risk management a priority.** Have a discussion about the new fraud guidance involving your senior management, board of directors, and audit committee to garner top-level support. Build a cross-departmental fraud risk management committee. Talk about fraud risks and how organizations can benefit by enhancing their fraud risk management capabilities and share examples of fraud schemes in the news or from your organization's past intelligent risk management comes with openness and awareness.

- **Perform a gap analysis.** Compare your organization's fraud risk management practices with those recommended in the new guidance. Identify the missing elements and determine priorities for how these gaps should be addressed. For those practices your organization already has in place, use the leading practices suggested in the guidance to help uncover further performance improvement opportunities. Some organizations find a scorecard or a simple "red, yellow, green" rating system efficient and effective.

- **Plan and execute a fraud risk management program.** Establish clear roles, responsibilities, and accountability for fraud risk management. Set goals and timelines and measure your progress in implementing improvements. Put an annual process in place to update the fraud risk assessment and re-evaluate your fraud risk management plan based on changes in the risk environment. Some executives find a "dashboard" approach helpful for monitoring and sharing information about their program.

Fraud Risk Management Cycle



Contacts

Neeta Potnis
E-mail: neetapotnis@deloitte.com
Tel:+91 (22) 6667 9000

Nitin Khanapurkar
E-mail: nkhanapurkar@deloitte.com
Tel:+91 (22) 6681 0700

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.