PUBLISHED BY THE INSTITUTE OF INTERNAL AUDITORS

TONE at the TOP

Issue 40 August 2008

EXCLUSIVELY FOR SENIOR MANAGEMENT, BOARDS OF DIRECTORS, AND AUDIT COMMITTEES

Combating the Risky Business of Fraud

No organization is exempt from fraud risks. Large frauds have led to the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets. Publicized fraudulent behavior by key executives has negatively impacted the reputations, brands, and images of many organizations around the globe.

Regulations such as the 1977 U.S. Foreign Corrupt Practices Act, the 1997 Organization for Economic Cooperation and Development Anti-Bribery Convention, the U.S. Sarbanes-Oxley Act of 2002, the 2005 U.S. Federal Sentencing Guidelines, and similar legislation throughout the world have increased management's responsibility of fraud risk management.

Reactions to recent corporate scandals have led the public and stakeholders to expect organizations to take a "no-fraud-tolerance" attitude. Good governance principles demand that the board or equivalent oversight body ensures ethical behavior regardless of the organization's status, sector, size, or industry. Surprisingly enough, historical records indicate that most major frauds are perpetrated by senior management in collusion with other employees. Vigilant handling of fraud cases within an organization sends clear signals to the public, stakeholders, and regulators about the attitude of those at the top — management and the board — toward fraud risks.

Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

Only through diligent and ongoing efforts can an organization protect itself against significant acts of fraud. Recently, The Institute of Internal Auditors (IIA), the American Institute of Certified Public Accountants (AICPA), and the Association of Certified Fraud Examiners (ACFE) produced "Managing the Business Risk of Fraud: A Practical Guide," which delineates five principles for boards and management to consider as they attempt to protect their organizations from fraud.

All levels of personnel throughout the organization, including management, staff, internal auditors, and external auditors have responsibility for dealing with fraud risk. Based on its size and circumstances, each organization should assess the degree of emphasis to place on fraud risk management. However, everyone in the organization should understand and be able to answer these questions:

- *How is the organization responding to heightened regulations and close scrutiny by the public and the stakeholders?*
- *What form of fraud risk management program does the organization have in place?*
- *How does the organization identify fraud risks?*
- *What is being done within the company to better prevent fraud, or at least detect it sooner?*
- *What process is in place to investigate fraud and take corrective action?*

Principle 1: As part of an organization's governance structure, a fraud risk management program should be in place, including a written policy or policies to convey the expectations of the board of directors and senior management regarding managing fraud risk.

Stakeholders clearly have raised expectations for ethical organizational behavior, while regulators worldwide have increased criminal penalties that can be levied against organizations and individuals who participate in committing fraud. Organizations should respond to such expectations, by ensuring that effective governance processes — the foundation of fraud risk management — are in place. Lack of effective corporate governance seriously undermines any fraud risk management program. The overall tone at the top sets the organization's tolerance of fraud.

The board of directors should ensure that its own governance practices set the standard for managing the risks of fraud, and that management implements policies that encourage ethical behavior. These policies should include a process that employees, customers, and vendors can follow to report fraudulent or unethical behavior. The board also should monitor the organization's fraud risk management effectiveness, making the topic a regular item on its agenda. To this end, the board should appoint one executive-level member of management to be responsible for coordinating fraud risk management and reporting those activities to the board.

Most organizations have activities and some form of written policies and procedures to manage fraud risks. However, few have developed a concise summary of activities or documents designed for communicating and evaluating these activities. While each organization needs to consider its size and complexity when determining appropriate formal documentation, a fraud risk management program should comprise the following:

- *Board and organizationwide commitment to fraud risk management.*
- *Fraud awareness.*
- *Periodic affirmation process.*
- *Conflict disclosure.*
- *Fraud risk assessment.*
- *Reporting procedures and whistleblower protection.*
- *Investigation process.*
- *Corrective action.*
- *Quality assurance.*
- *Continuous monitoring.*
- *Roles and responsibilities.*

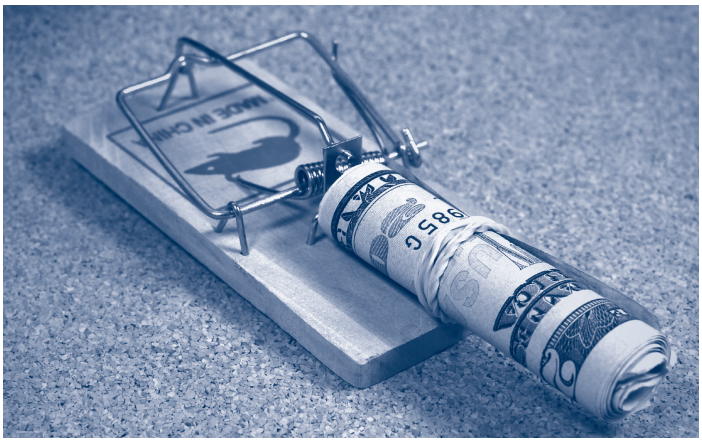
Principle 2: Fraud risk exposure should be assessed by the organization to identify potentially fraudulent schemes and events.

To effectively and efficiently protect itself and its stakeholders from fraud, an organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization. A structured fraud risk assessment — tailored to the organization's size, complexity, industry, and goals — should be performed and updated periodically. The assessment may be integrated with an overall organizational risk assessment or a stand-alone exercise. It should, at a minimum, include risk identification, risk likelihood and significance assessment, and risk response.

Fraud risk identification may include gathering external information from regulatory bodies, industry sources, key guidance-setting groups, and professional organizations. Internal sources for identifying fraud risks should include interviews and brainstorming with personnel representing a broad spectrum of activities within the organization, review of whistleblower complaints, and analytical procedures.

An effective fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. Employee incentive programs and the metrics on which they are based can provide a blueprint for where fraud is most likely to occur. Fraud risk assessment should consider when management might potentially override controls, which controls are weak, and where duties are not segregated.

Assessing the likelihood and significance of each potential fraud risk is a subjective process that should consider not only monetary significance, but also significance to an organization's financial reporting, operations, reputation, and legal and regulatory compliance requirements. An initial assessment of fraud risk should consider the inherent risk of a particular fraud in the absence of any known controls that may address the risk.



Individual organizations have different risk tolerances. Fraud risks can be addressed by establishing practices and controls to mitigate the risks, accepting the risks — but monitoring actual exposure — or designing ongoing or specific fraud evaluation procedures to deal with individual fraud risks. An organization should strive toward taking a structured approach versus a haphazard approach. The benefit an implemented fraud risk management program provides should exceed its cost. Board members should ensure that the appropriate "control mix" is in place, recognizing their oversight duties and responsibilities in terms of the organization's sustainability and their fiduciary role to stakeholders. Management is responsible for developing and executing mitigating controls to address fraud risks while ensuring controls are executed efficiently by competent and objective individuals.

Principle 3: Prevention techniques to avoid potential key fraud risk events should be established as feasible to mitigate possible impacts on the organization.

Fraud prevention and detection are related, but not the same. Prevention encompasses policies, procedures, training, and communication activities that stop fraud from occurring. Detection, however, focuses on activities and techniques that recognize, in a timely manner, whether fraud has occurred or is occurring.

While preventive techniques do not ensure an organization is exempt from fraud, they are the first line of defense in minimizing fraud risk. One key to prevention is building throughout the organization and its governance structure an awareness of the fraud risk management program and the types of fraud that could potentially occur.

Principle 4: Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized.

One of the strongest fraud deterrents is the awareness that effective detective controls are in place. Combined with preventive controls, detective controls enhance the effectiveness of a fraud risk management program by showing that controls are working as intended to identify fraud if it occurs. Although detective controls may provide evidence that fraud has occurred or is occurring, they are not intended to prevent fraud.

Principle 5: A reporting process should be in place to solicit inputs on potential fraud and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is appropriately dealt with in a timely manner.

No system of internal control can provide absolute assurance against fraud. As a result, the board should ensure the organization develops a system for prompt, competent, and confidential review, investigation, and resolution of allegations involving potential fraud. The board also should define its own role in the investigation process. An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation, by establishing and preplanning investigation and corrective action processes.

The board and the organization should establish a process to evaluate allegations. Individuals assigned to investigations should have the necessary authority and skills to evaluate the allegation and determine the appropriate course of action. The process should include a tracking or case management system where all allegations of fraud are logged. Clearly, the board should actively be involved with respect to allegations involving senior management.

If further investigation, beyond evaluation, is deemed the appropriate next course of action, the board should ensure that the organization has an effective process to investigate cases and maintain confidentiality over the process. A consistent process for conducting investigations can help the organization mitigate losses and manage risk associated with the investigation. In accordance with policies approved by the board, the investigation team should report its findings to the appropriate party, such as senior management, directors, legal counsel, and oversight bodies. Public disclosure also may need to be made to law enforcement, regulatory bodies, investors, shareholders, the media, and others.

If certain actions are required to preserve evidence, maintain confidence, or mitigate losses before the investigation is complete, those responsible for such decisions should ensure there is sufficient basis for those actions. When access to computerized information is required, specialists trained in computer file preservation should be used. Actions taken should be appropriate under the circumstances and applied consistently to all levels of employees, including senior management. They should be taken only after consultation with individuals responsible for such decisions and human resources. Consulting legal counsel also strongly is recommended before undertaking an investigation and is critical before taking disciplinary, civil, or criminal action.

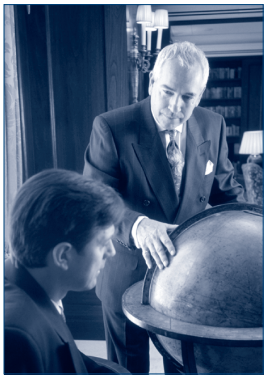
As a matter of good governance, the board should ensure that appropriate risk fraud management measures are in place. After all, fraud is risky business that can bring an organization to its knees.

NOTE: To request a link to the full fraud paper, contact PR@theiia.org.

TONE at the TOP

The Institute of Internal Auditors
247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA

TONE at the TOP



Mission

To provide executive management, boards of directors, and audit committees with concise, leading-edge information on such issues as ethics, internal control, governance, and the changing role of internal auditing; and guidance relative to their roles in, and responsibilities for, the internal audit activity.

Your comments about *Tone at the Top* are welcomed.

Director, Corporate Communications and PR:
Trish W. Harris, trish.harris@theiia.org
+1-407-937-1245

Complimentary Subscriptions Available

You, your colleagues, and your audit committee and board members are invited to receive complimentary subscriptions to *Tone at the Top*. Send your request for printed or electronic versions of the newsletter to **pr@theiia.org** or write to us at:

The Institute of Internal Auditors
Corporate Communications
247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA
Fax: +1-407-937-1101

Tone at the Top is also archived online. All issues are available on **www.theiia.org** in the "Newsletters" section under "Periodicals."

To reprint, translate, or post this edition of *Tone at the Top*, contact pr@theiia.org.

The Institute of Internal Auditors (www.theiia.org) is dedicated to the global promotion and development of internal auditing.

Established in 1941, The IIA is an international professional association with global headquarters in Altamonte Springs, Fla. The IIA has more than 150,000 members in internal auditing, risk management, governance, internal control, IT auditing, education, and security.

The IIA is the global voice, recognized authority, chief advocate, principal educator, and acknowledged leader in certification, research, and technological guidance for the internal audit profession worldwide. The IIA enhances the professionalism of internal auditors and is internationally recognized as a trustworthy guidance-setting body. It fosters professional development, certifies qualified audit professionals, provides benchmarking, and through The IIA Research Foundation, conducts research projects and produces educational products.

08/08025 bsp
Printed in the U.S.A. on recycled paper.