

RECOGNITION OF THE ANTI-FRAUD PROFESSION

Discipline emerging as true profession

By Dr. Haluk F. Gursel, CFE, CGFM, CPA

Global firms are realizing that the anti-fraud profession, led by Certified Fraud Examiners, is an important component of risk measurement and avoidance. Learn how recent risk-based management control systems are hastening the development of specialized anti-fraud agents.

George, the new CEO of a medium-sized manufacturer, wasn't sure he needed two Certified Fraud Examiners on staff. Hadn't the internal audit department sufficiently protected the firm against risk in the past? But then his auditors discovered some irregularities in the procurement department and the CFEs were called in. They eventually found that David, the acquisitions manager, had been building his stable of loyal vendors for years by soliciting kickbacks.

George was sold. He hired two additional CFEs who also work with internal audit to detect and deter fraud and conduct fraud examinations.

The case is fictitious but it's indicative of many firms throughout the globe that are recognizing that the emerging anti-fraud profession is integral to measuring and avoiding risk.

CEOs only have to read the ACFE's 2006 "Report to the Nation," which estimates that the typical U.S. organization loses 5 percent of its annual revenues to fraud, to begin to understand the magnitude of the problem. Applied to the 2006 U.S. Gross Domestic Product, this translates to approximately \$652 billion in total losses. Management has to acknowledge the overall consequences of the fraud risk and fraud itself.

Joseph T. Wells, CFE, CPA, founder and Chairman of the ACFE, has said, "fraud is not an accounting problem; it's a social phenomenon." After management has its "anti-fraud epiphany," it can devise its strategies. Here we'll describe the changing roles and functions of CFEs and other anti-fraud professionals and how they can work together with internal audit departments and management.

MAJOR DYNAMICS IN THE FIELD

In the early part of the 20th century, the work related to anti-fraud activities (awareness, prevention, detection, and examination) was entrusted to audit professionals. Auditors, with their vast accounting knowledge, took jobs in the field of suspected or attempted organizational fraud cases. The fraud risk (the conditions that can allow fraud to occur) was mitigated by the use of an auditor's knowledge.

The 21st century, however, is witnessing two major changes. On one hand, fraudsters are becoming more sophisticated and, therefore, harder to beat. On the other hand, a new breed of specialized professionals in the field of fraud examination is emerging. Many are realizing that

pure knowledge of accounting isn't sufficient to deal completely with fraud-related problems.

Recent risk-based management control systems are hastening the development of specialized anti-fraud agents. In this issue and the next, we'll review the risk management cycle, the fraud risk, and functions of anti-fraud professionals and explain why they're in such demand.

RISK MANAGEMENT CYCLE

An organization conducts a risk management cycle (shown in Figure 1) by:

1. identifying risk areas;
2. understanding and assessing scale of risk;
3. developing risk management strategy;
4. implementing strategy and allocating responsibility;
5. implementing and monitoring implementation of controls; and
6. establishing risk management group and goals

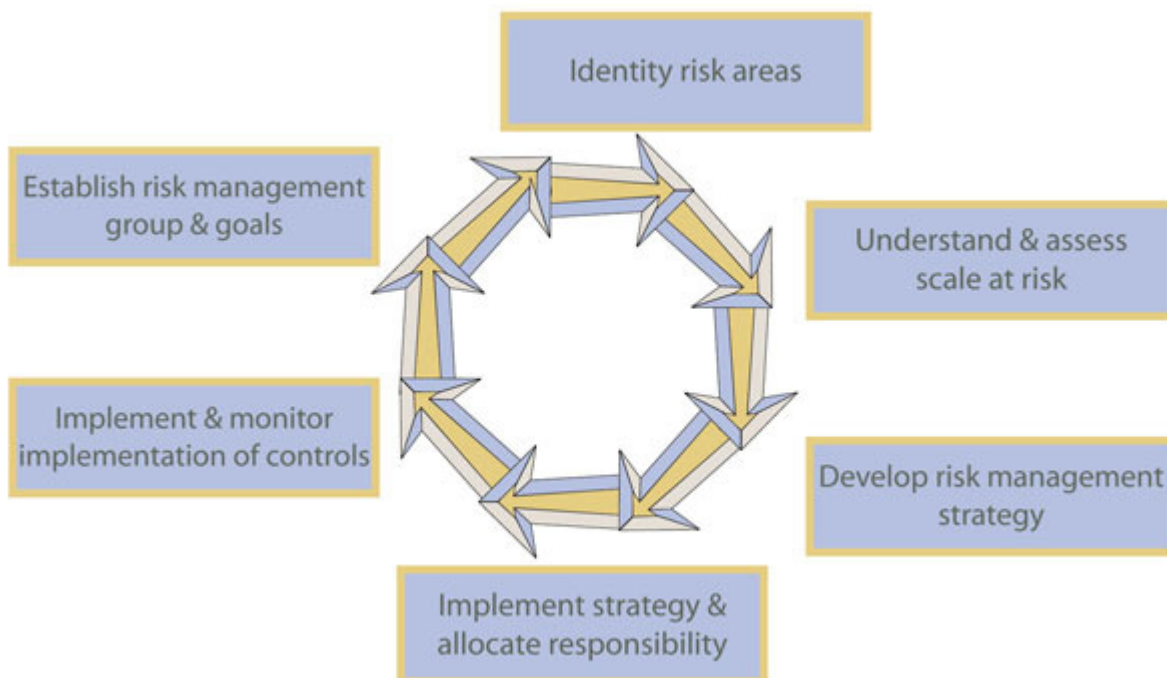


Figure 1: Risk management cycle

ENTERPRISE RISK MANAGEMENT

The risk management cycle is best examined by using the 2004 Enterprise Risk Management (ERM) Framework produced by the Committee of Sponsoring Organizations of the Treadway Commission. According to its main document, "Enterprise Risk Management – Integrated Framework," Enterprise Risk Management is:

- a process, ongoing and flowing through an entity;
- effected by people at every level of an organization;
- applied in strategy setting;
- applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk (consideration of interrelated risks at the organization level);
- designed to identify potential events that, if they occur, will affect the entity and to

manage risk within its risk appetite (the amount of risk an organization is willing to absorb to attain the objectives it wants);

- able to provide reasonable assurance to an entity's management and board of directors; and
- geared to achievement of objectives in one or more separate but overlapping categories.

Enterprise Risk Management encompasses:

Aligning risk appetite and strategy – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events, establish responses, and reduce surprises and associated costs or losses.

Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts and integrated responses to these risks.

Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

This enterprise-wide risk management framework is geared to achieve an entity's objectives, set forth in four categories:

Strategic: high-level goals, aligned with and supporting its mission;

Operations: effective and efficient use of its resources;

Reporting: reliability of reporting; and

Compliance: compliance with applicable laws and regulations.

Finally, Enterprise Risk Management consists of eight interrelated components. These are derived from the ways management runs an enterprise and are integrated with the management process:

Internal environment – This encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's employers and employees including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

Objective setting – Objectives must exist before management can identify potential events that might affect their achievement. Enterprise Risk Management ensures that management has a process in place to set objectives, which support and align with the entity's mission. These objectives must also be consistent with the company's risk appetite.

Event identification – Internal and external events that will affect the achievement of an entity's objectives must be identified. Risks and opportunities must be distinguished. Opportunities will be

channeled back to management's strategy or objective-setting processes.

Risk assessment – Likelihood and impact are used as bases for analyzing risk and determining how it should be managed and assessed inherently and residually.

Risk response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – when developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

Control activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Information and communication – Relevant information is identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication flows down, across, and up the entity's organizational chart.

Monitoring – The entirety of Enterprise Risk Management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

RESPONSIBILITY FOR FRAUD RISK

The fraud position statement of the Institute of Internal Auditors UK and Ireland widely accepts the risk management model of COSO.2 In its dynamic version of the ERM Framework, the institute states that each organization should:

- set the tone from the top by having a policy that makes it clear that fraud won't be tolerated, fraudsters will be prosecuted, and the organization is committed to preventing and detecting fraud.);
- have a risk management strategy that includes fraud risk mitigation measures, which are aimed at detecting fraud and deterring would-be fraudsters;
- have a fraud response plan that states exactly the steps to take if a fraud is reported or detected; and
- have a continuous program of fraud awareness and regular updates and training for new and existing staff.

Thus, fraud is a risk like any other confronted by an entity. Therefore an entity's reaction to a fraud-related issued will be shaped by the risk response of that entity.

The primary responsibility for the prevention, detection, and investigation of fraud rests with management, which also has the responsibility to manage the risk of fraud. Many entities now have dedicated in-house "security" functions, which in addition to other tasks, manage fraud investigations and other fraud-related tasks such as awareness or prevention programs. Obviously, management has to hire qualified people to perform these tasks.

The internal audit department can assist in managing the fraud risk function. In fact, we consider this a compromise if internal auditors don't work with fraud examiners. If all entities don't fully understand the emerging anti-fraud profession, then an entity will never have enough qualified professionals to cope with all the anti-fraud tasks. Once the profession reaches its cruising altitude, we expect that an internal auditor's fraud-related tasks will change from fraud examination to the appraisal of anti-fraud processes such as evaluating programs devised by anti-fraud professionals.

CHIEF RISK OFFICER

In a perfect corporate world, a chief risk officer (CRO) or other anti-fraud professional would assist management in managing, controlling, reporting, and taking action on the risk of fraud by:

- establishing programs to increase awareness about fraud;
- devising processes to deter and detect fraud;
- applying adequate controls to prevent fraud;
- leading fraud investigations;
- overseeing investigations conducted by specialists on their behalf;
- dealing effectively with issues raised by staff (including taking appropriate action to deal with reported or suspected fraudulent activity); and
- involving the police when necessary.

In the next issue: differences between internal auditors and fraud examiners, management of anti-fraud programs and controls, role of the anti-fraud professional, and more.

Dr. Haluk F. Gursel, CFE, CGFM, CPA, is the president of the Switzerland Chapter of the ACFE. He has been an anti-fraud specialist since 1967; is an adjunct professor at Webster University in Geneva, Switzerland; and is the author or contributor of and to numerous books and articles. Gursel was an advisor in drafting the "United Nations Fraud Prevention and Anti-Corruption Framework." He is helping upgrade the Pan American Health Organization Oversight Department. His e-mail address is: gursel@yahoo.com.

1 Adapted from "Managing the Risk of Fraud – A Guide for Managers." Public Enquiry Unit, HM Treasury, London. 1997.

2 Institute of Internal Auditors UK and Ireland. "Fraud Position Statement." April 2003.

The Association of Certified Fraud Examiners assumes sole copyright of any article published in Fraud Magazine. Fraud Magazine follows a policy of exclusive publication. Permission of the publisher is required before an article can be copied or reproduced. Requests for reprinting an article in any form must be e-mailed to: FraudMagazine@ACFE.com.