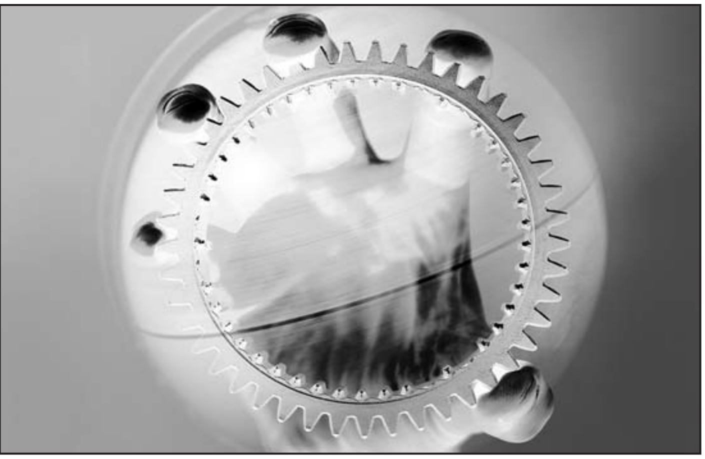
# Risk Management Newsletter

March 2006 – Issue No. 7

# Internal Controls—The COSO Way

by Dorothy L. Andrews

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was started by professionals from the following five professional organizations: The American Accounting Association, The American Institute of Certified Public Accounts, The Financial Executives Institute, The Institute of Internal Auditors, and The Institute of Management Accountants. Actuaries like to think of COSO as a euphemism for accountants taking over the world, especially in view of its sponsorship. The COSO has as its primary goal the improvement of corporate financial reporting, which makes it a stronghold in the emerging practice of Enterprise Risk Management.



The COSO published *Internal Control—Integrated Framework*, in 1992 in response to recent corporate scandals and audit improprieties. It should not be a surprise to anyone that business scandals lead to increased regulations. The Security and Exchange Commission (SEC) and the National Association of Insurance Commissioners (NAIC) have as their mission to protect consumer interests from the effects of corporate misconduct. Their only weapons are legislation and regulation, but they are aimed at the good, the bad, and the ugly alike. Paradoxically, the SEC and the NAIC, in effect, contribute to the erosion of consumer value because the burden of increased legislation and regulation challenge the best and biggest of companies to survive profitably under tough economic and regulatory conditions. The COSO principles of internal control are intended to be self-policing, by providing a framework to place under surveillance the activities of key areas of a company. A surveillance system should link key activities across an organization and illustrate the impact on the organization of a failure in a key activity. For example, if policies error from a reserve valuation run, then the surveillance system should capture the missing policies and trigger an alert to indicate, at the very minimum, that the number of policies valued does not agree with the policy count of the valuation file. While more complicated alerts are possible and appropriate, it was rare to find insurers with this simple model in place to validate reserves in my many years of performing actuarial audits on insurance companies.

The new approach to risk management as embodied in the COSO principles looks at organizational risk from a broader perspective than would traditional risk management. Traditional risk management was purely concerned with the frequency and severity of expected losses. The new risk management paradigm has a much wider wingspan and circles over a much wider landscape of an organization with its internal control doctrines. The COSO defines internal control as *a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: 1) Effectiveness and efficiency of operations, 2) Reliability of financial reporting, and 3) Compliance with applicable laws and regulations.* It is important to understand the fundamental concepts upon which this definition rests. *First, internal control is a process, a means to an end, not an end in itself. Second, internal control is effected by people. It is not merely policy manuals and forms, but people at every level of the organization. Third, internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board. Fourth, internal control is geared to the achievement of objectives in one or more separate, but overlapping categories.*

Let's examine briefly each of these fundamental concepts.

Dorothy L. Andrews, ASA, MAAA, is vice president of the risk management department of Wachovia Corporation in Charlotte, N.C. She can be reached at *Dorothy.Andrews@ wachovia.com.*

## Process

The most important thing to understand about internal control is that it is a management tool consisting of a network of business activities that are not only inter-related, but also reactive to negative stimuli within the network. This network extends to and is ingrained in every corner of the organization, making it as much of the essence of the organization as that expressed by the organization's mission statement. In this way, internal control is not intended to relieve management of an active and participatory role in running the business or the responsibility of adverse consequences of business activities.

The COSO way describes internal controls as "built-ins" rather than "built-ons" to an organization's infrastructure. The difference is that built-in controls are internal to a process, while built-on controls are external to a process. For example, enabling valuation systems to programmatically verify policy counts and premiums against financial ledger amounts is an example of a built-in control. In this scenario, discrepancies are highlighted immediately and appropriate actions can be taken. A built-on control would involve a manual reconciliation of the two files, which, depending on resources, may or may not get done. Built-in controls are the handmaidens to effective quality initiatives, aiding in the containment of the cost of doing business and decreasing reaction time to adverse events.

## People

We all know the cliché, "Our people are our greatest asset," or something similar. These assets, however, can erode company value if ill-trained to perform as needed. Internal control is implemented by every member of the organization, from the board members to the receptionists and security guards. They all have a role to play in effecting sound internal control management. Most people in an organization do not understand the impact their jobs have on the work productivity of others. For this reason, it is important to train associates at all levels of an organization in the principles of risk management. The principles emphasize the impact and inter-relationships among firm activities.

Information is a most valuable asset in a company and senior management depends on high quality information to steer the organization in a profitable direction. However, the flow of information in many organizations is a lot like playing the familiar, childhood telephone game. In the telephone game, a message is whispered from one person to the next until it gets to the last person in the line. The last person stands up and recites the message and a comparison is made to the content of the message whispered by the first person in the line. With near perfect probability, the recitation made by the last person has no relationship to the content of the initial message whispered. This game epitomizes the flow of information in most insurance companies with senior management as the final stop. The installation of a sound set of internal controls will improve the handoff of information around the organization, and empower management to better manage the company. Key to installing internal controls is an associate education program, which focuses on the interplay and impact of activities conducted throughout the organization. At the very minimum, risk management education should begin with new hires and then extend to others with the goal of changing the current culture to a more risk-conscious one.

## Reasonable Assurance

An organization may not succeed with internal controls, but it clearly cannot survive without them. They are not absolute in the preventing management from navigating the organization in the wrong direction, however. By their very nature, internal controls have limitations, as it is nearly impossible to manage for every operational and enterprise contingency. But, internal control systems do allow for retrofitting and upgrading as an organization sees fit to narrow the range of events that can nudge it off course. This

continued on page 12 ◗

> "The difference is that built-in controls are internal to a process, while built-on controls are external to a process."

## Internal Controls—The COSO Way

◗ continued from page 11

implies there must always be someone on watch and ready to react to adverse indicators triggered by the system.

## Objectives

Company objectives generally fall into one of three categories: operations, financial reporting, and compliance. Operational objectives include all those objectives relating to the effective and efficient use of firm resources. Financial objectives relate to the preparation of financial statements. And compliance objectives relate to compliance with laws and regulations. Operational objectives differ from the other two in that the achievement of the latter two objectives can be measured by external means. For example, either a company is compliant with a law or it is not. Operational objectives come in two flavors: internal and external. The achievement of internal operational objectives is subject to the people and processes of an organization. External operational objectives are not always within complete and total control of the organization. For example, the achievement of a specified investment return is not in the sole control of management. The internal control infrastructure should be responsive in measuring the fit or lack of fit between external organizational objectives and unfolding experience.

It should be recognized that an organization's objectives may fall into more than one category to address different needs and assign accountability for meeting those objectives to different officers of the company. The overlap should not prevent a reasonable assignment of expectations in meeting each category of objectives.

## The Five Components of Internal Control

The COSO has defined internal control as consisting of the following five components: control environment, risk assessment, control activities, information and communication, and monitoring. Each of these components is worthy of more attention than the treatment given here. However, a coloring of the role of each component in building an effective internal control system is important to complete this discussion.

Under COSO, a control environment is the sum total of the people making up the organization. Their integrity, ethical values, and competence are the main drivers of a company's success or failure. Education becomes key in making sure each member of an organization understands the risk culture management values and in making sure all members understand the required competencies required for their role.

The risk assessment function on a basic level identifies, analyzes and manages related risks. On a higher level, risk assessment involves the integration of risk recognition with objectives related to sales, production, marketing, financial and other activities. This integration should enable all these activities to work in tandem to maximize company value.

Control activities consist of the policies and procedures that monitor the execution of management directives. These activities come in many different forms depending on the directive. Approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties are among the types of control activities supported by a system of internal control. They are designed to prevent intentional and unintentional breaches of the risk policy of an organization.

It is universally agreed that the delivery of quality information is the central ingredient to good decision making. The COSO recognizes all the sources of both internally and externally generated data and supports a complete inventory of such to define the inter-relatedness of all the pieces. These inter-relationships form the basis of a risk management surveillance system and are integral to an internal control process. The communication to and education of associates further cements the importance of the roles performed by others and the impact of these various roles in concert and in isolation.

Lastly, the ever important activity of monitoring is a necessary evil to ensure the process in working as desired. Periodic evaluations are necessary to flag irregularities in the system. The scope and frequency of these activities is a function of the degree to which manual processes are involved. More manual tasks naturally become candidates for more monitoring to maintain equilibrium in the system. It is important to report imbalances upstream for immediate resolution to empower management to adjust the course of the organization toward a more profitable direction.

In summary, installing internal controls is no small task. Many organizations have antiquated systems and depend on manual processes controlled by people to understand the organizational mechanics that drive bottom line results. It also becomes very challenging to assess how and when pertinent data adversely changes form or if it has changed at all. Maintaining data integrity as data flows throughout the organization must be a top priority and a key objective in designing an internal control process. A second priority and design incentive must be the alignment of individual goals with company objectives. History has shown us that a misalignment is often the root cause for the deterioration of company value. It is more true than not that the likelihood of a catastrophe event bringing down an organization is much, much smaller than that of mismanagement. Therefore, if an organization needs two reasons for installing internal control processes, then maintaining data integrity and preventing mismanagement are very strong ones.

Required reading for all risk officers: *Internal Control—Integrated Framework*, September, 1992 and *Enterprise Risk Management—Integrated Framework*, September, 2004, by the Committee of Sponsoring Organizations of the Treadway Commission. Both are available from the American Institute of Certified Public Accountants (*www.aicpa.org*) for less than one business scandal or one faulty audit. ✦

> “History has shown us that a misalignment is often the root cause for the deterioration of company value.”