

Managing Risk from the Mailroom to the Boardroom

Few areas of corporate oversight are more important these days than the evaluation of the organization's ability to manage risk. However, risk and control are virtually inseparable — like two sides of a coin — meaning that risks first must be identified and assessed; then managed and mitigated by the implementation of a strong system of internal control.

Although top organizations have long shared with their stakeholders their commitment to and steps toward ensuring strong internal controls, the Sarbanes-Oxley Act of 2002 made reporting on internal control a requirement. Specifically, Section 404 requires publicly held companies to include in their annual report a certification from management that the company has established internal controls for its financial reporting process. In addition, the SEC issued a rule indicating that a control framework must be used and identified.

For years, organizations reflecting best practices have depended on The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Internal Control Integrated Framework* as the model upon which they have built a strong system of internal control. Today more than ever, those at the top of their organization depend on this and other frameworks to ensure appropriate assignment of roles and responsibilities in regard to the control environment, risk assessment, control activities, information, communication, and monitoring.

Once again, COSO — comprising the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, The Institute of Internal Auditors, and the Institute of Management Accountants — is stepping

forward, and not a moment too soon, with a framework that meets the needs of the day.

Enterprise risk management (ERM) is the process of identifying and analyzing risk from an integrated, companywide perspective. Scheduled for exposure in July and due for release in early 2004, COSO's *ERM Framework* will offer boards and management — regardless of the organization's size or scope — a commonly accepted model for discussing and evaluating the organization's risk management efforts. This includes all activities geared toward meeting its strategic, operational, reporting, and compliance objectives. The framework will focus on the necessity of a consistent "risk and control consciousness" throughout the enterprise; the importance of considering risk during the formulation of strategy; and the interrelationships of risks across business units and at every level of the organization.



From the internal auditor's perspective, ERM is significantly different than more traditional risk management approaches. Auditors have long honed in on specific activities independent of other functions within the organization.

Through ERM, however, there is great potential for accurately assessing risk on a big-picture, enterprisewide scale. This is especially significant, as the internal auditors' primary mission is to help management and the board to achieve their objectives.

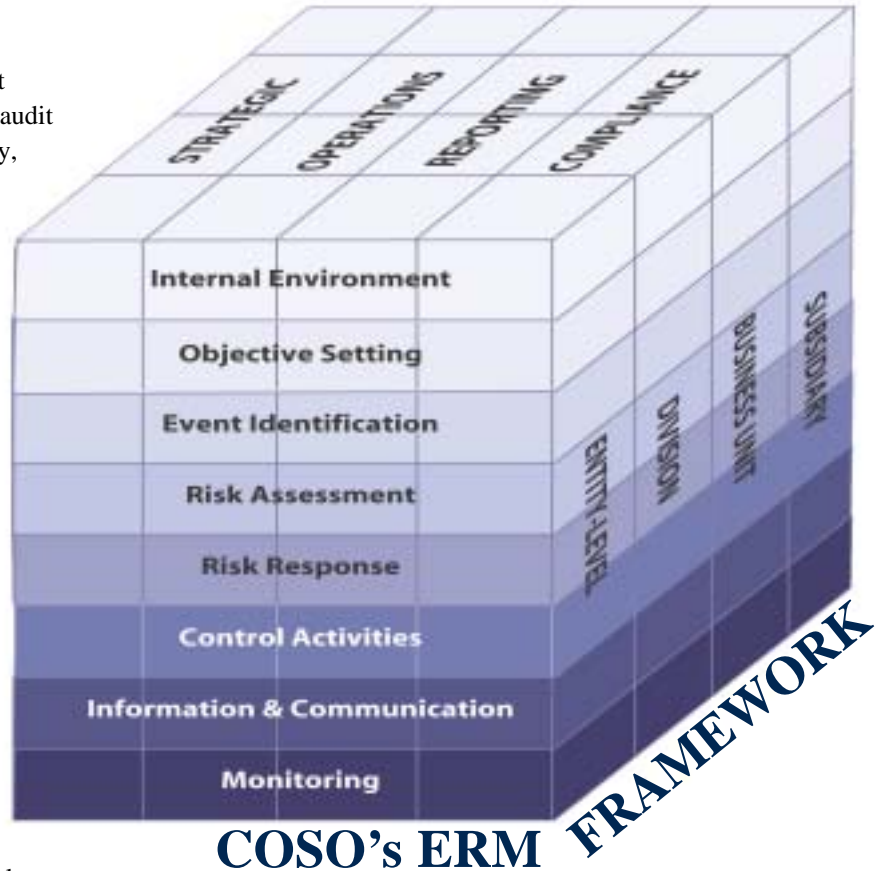
Parallel to the greater ERM movement, the internal audit function has undergone a transformation to a risk-based audit approach. In The IIA Research Foundation's recent study, *Enterprise Risk Management: Pulling It All Together*, the authors examine the role of internal audit in ERM implementation in five different types of organizations: the electric utility industry, manufacturing, retailing, oil and gas operations, and the public sector.

This groundbreaking research report demonstrates how ERM can help organizations focus the efforts of employees on the most important issues and boost stakeholder value. The authors — Thomas L. Barton, Ph.D., CPA; William G. Shenkir, Ph.D., CPA; and Paul L. Walker, Ph.D., CPA — assert that ERM is most effective when the internal audit function plays a key role in its implementation, especially when management views the internal auditor as a key consultant, rather than a watchdog.

In the April 2003 *Internal Auditor* article, "Creating a Risk-intelligent Organization," Rick Funston asserts that for ERM to be implemented successfully, it must be "built into" rather than "bolted onto" management's planning and decision-making processes. Funston states that if ERM is seen solely as another initiative, it will fail. Rather, it must be perceived as management's way of doing business successfully.

As any adept leader knows, managing risk is something of a balancing act. Give a little here — take a little there. The

COSO ERM Framework allows for governance flexibility and judgment. It is based on eight key components: internal environment; objective setting; event identification; risk assessment; risk response; control activities; information and communication; and monitoring.



COSO's ERM

assessment; risk response; control activities; information and communication; and monitoring. Included in the framework is a mandate for coordination of all of these components for maximum effectiveness of the risk management process.

In 2002, The IIA conducted a survey that revealed a large percentage of board directors did not even know whether

ERM ENHANCES THE ORGANIZATION'S ABILITY TO:

- Align risk appetite and strategy.
- Link growth, risk, and return.
- Enhance risk response decisions.
- Minimize operational surprises and losses.
- Identify and manage cross-enterprise risks.
- Provide integrated responses to multiple risks.
- Seize opportunities.
- Rationalize capital.
- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.



their organizations had in place a risk management program. The framework is expected to be a useful tool for informing directors and other stakeholders about the processes and procedures in place to identify, measure, prioritize, and respond to risk. As a result, board members will be in a position to accurately measure how well their management teams are handling the risks they face.

Although the framework will

help organizations get on track with their risk management processes, it is important to acknowledge there's really no substitution for integrity and an organization-wide understanding that controls are everybody's business. The mindset that organizations are no stronger than their weakest link or most ineffective process, points to the importance and value of strong systems of internal control and comprehensive risk management programs, supported by an ethical tone at the top and high-road corporate culture. Step one is simple: to hire only highly principled employees.

Every entity, whether for-profit or not, exists to realize value for its stakeholders. Value is created, preserved, or eroded by management decisions in all activities, from setting the strategy to operating the enterprise on a day-to-day basis. ERM supports value creation.

In the words of esteemed economist Frank Knight, the paradox of risk is that it results from the future being different from the past, while traditional risk management relies upon the future being similar to the past. Modern organizations cannot absolve themselves from responsibility for disaster by saying that they didn't anticipate an event because it had never happened before. Risk assessment must be pervasive and diligent. Managers must understand and acknowledge all potential risks and have action plans in place to mitigate them. And internal auditors must play a proactive role in the ERM team.

The ERM Framework exposure draft will be available for comment after July 15 at www.coso.org.

ERM QUESTIONS Management and the Board Should Consider

- What is the organization's risk management philosophy?
- Is that philosophy clearly understood by all personnel?
- What are the relationships among ERM, performance, and value?
- How is ERM integrated within organizational initiatives?
- What is the desired risk culture of the organization and at what point has its risk appetite been set?
- What strategic objectives have been set for the organization and what strategies have been or will be implemented to achieve those objectives?
- What related operational objectives have been set to add and preserve value?
- What internal and external factors and events might positively or negatively impact the organization's ability to implement its strategies and achieve its objectives?
- What is the organization's level of risk tolerance?
- Is the chosen risk response appropriate for and in line with the risk tolerance level?
- Are appropriate control activities (i.e., approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, segregation of duties) in place at every level throughout the organization?
- Is communication effective — from the top down, across, and from the bottom up the organization?
- How effective is the process currently in place for exchanging information with external parties?
- What is the process for assessing the presence and performance quality of all eight ERM components over time?

TONE_{at}theTOP 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 function.

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

Assistant VP, Corporate Marketing & PR:
Trish W. Harris, tharris@theiia.org
+1-407-937-1245

Complimentary Subscriptions Available

You and your colleagues and audit committee and board members are invited to receive complimentary subscriptions to *Tone at the Top*. Send your requests for printed copies or e-mail notification when new issues are available to pr@theiia.org or mail them to:

The Institute of Internal Auditors
Corporate Marketing & PR
247 Maitland Avenue
Altamonte Springs, FL 32701-4201 USA
Fax: +1-407-937-1101

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

 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, FL. The IIA has more than 85,000 members in internal auditing, risk management, governance, internal control, IT audit, education, and security.

The Institute is the recognized authority, principal educator, and acknowledged leader in certification, research, and technological guidance for the profession worldwide. The IIA presents conferences and seminars, produces educational products, certifies qualified audit professionals, provides quality assurance reviews and benchmarking, and through The IIA Research Foundation, conducts research projects.