The Institute of Internal Auditors

TONE at the TOP

Issue 55 | June/July 2012

Exclusively for Senior Management, Boards of Directors, and Audit Committees

Strong Links for Effective Risk Management

As the saying goes, *a chain is only as strong as its weakest link*. This adage rings true in many situations. In regard to risk, for example, there are countless points at which various individuals might contribute to the overall strength of an organization's management of risk. The antithesis of the "it's-not-my-job" mentality, this mindset is all about a corporate consciousness of risk, people stepping up and assuming responsibility, and those at the top doing everything possible to ensure personal and collective accountability throughout the enterprise.

Who's responsible for risk?

Through the years, guidance on risk management has been issued by a variety of organizations around the world such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO); the International Organization for Standardization (ISO); the Information Systems Audit and Control Association (ISACA); the Risk Management Society (RIMS); and the Federation of European Risk Management Associations (FERMA). Risk management principles have evolved to help organizations build strong risk management programs. For example, in 2004 COSO published *Enterprise Risk Management–Integrated Framework*. This well known framework established common definitions, provided direction for enhancing risk management, and set criteria for evaluating whether a risk management program is effective.

In addition to building a risk management program around a framework like COSO's, many thought leaders believe that risk management, at its best, is a shared philosophy with shared responsibility. Over the years, *Tone at the Top* frequently has pointed out that controls are *everybody's business*. Likewise, risk management is *everybody's responsibility*.

As line management considers the various decisions they face daily, risk should be on their radar…and the controls, policies, and procedures that would

minimize the likelihood of those risks materializing. Likewise at the top of the organization, boards and executive management must collaborate for risk management as they develop strategies. There is an opportunity for organizations to embed this process into their management culture. At the end of the day, the board and CEO are ultimately responsible for risk management. But it's only truly possible through a collective effort.

Functional Collaboration

So if, ideally, risk management is everybody's responsibility at every level of the organization and if all functions are attuned to its importance and its mandate, how can they work together for the greater good? What can specific areas do to coordinate their work with the efforts of others from a risk perspective?

Recently, The Institute of Internal Auditors (IIA) and RIMS released a joint report on the value garnered when the internal auditors and risk managers collaborate on risk management efforts. The report reflects the view of The IIA and RIMS that effective collaboration and open dialogue result in a more robust view of the entire risk portfolio.

"Risk managers and internal auditors have many of the same stakeholders — boards and executive management — and these stakeholders want to maximize resources while effectively managing risk," IIA Vice President of North American Services Hal Garyn, CIA, says in the report. "Having these vital risk management and assessment functions collaborate, speak the same language, and leverage one another's perspectives on the business is crucial."

Carol Fox, RIMS director of strategic and enterprise risk practice, agrees. "Risk management and internal audit roles are complementary. An overarching common goal is to position organizations for successful achievement of their respective missions and business objectives," Fox says in the report. "The two disciplines are more effective working together than separately, especially when there is a common understanding of each other's roles. For example, as the internal auditors offer assurance as to management's effectiveness regarding strategic risks, the risk management function provides the techniques and methods for management to be most effective."

The report, "Risk Management and Internal Audit: Forging a Collaborative Alliance," includes case studies of differing approaches at four risk-savvy organizations: Cisco Systems, Hospital Corporation of America (HCA), TD Ameritrade, and Whirlpool Corporation.

Common and effective collaborative practices that emerged during the case studies include:

- Linking the audit plan and the enterprise risk assessment, and sharing other work products to provide assurance that critical risks are being effectively identified.
- Sharing available resources wherever and whenever possible to allow for efficient use of scarce resources, such as finances, staffing, and time.
- Cross leveraging each function's respective competencies, roles, and responsibilities to provide communication depth and consistency, especially at the board and management levels.
- Assessing and monitoring strategic risks to allow for deeper understanding and focused action on the most significant risks.

According to the study, ERM results shared with internal audit can be factored into the audit plan. Also, when the internal auditors discuss their risk-based audit plan with the risk management team, valuable insights from different perspectives on organizational governance and enterprise oversight occur. These approaches help eliminate redundancies in identifying critical risks to the organization, produce a common and aligned view of the organization's risk profile, and help instill a consistent risk management vocabulary.

"In addition to integrating ERM risk considerations into our annual risk assessment process, an improvement we've introduced over the last few years is to show the linkage between the audits on our audit plan to the related primary ERM category. This linkage highlights in a tangible way the integration between the audit and risk management functions," Whirlpool's Irene Corbe says in the report. Corbe serves as vice president of internal audit at Whirlpool.

Open communication, even though the channels may vary, is a valuable component of all of the case studies. Some of the organizations studied conduct regularly scheduled in-person meetings. Others correspond in writing, some communicate by telephone, and most use multiple methods to exchange ideas and information.

Effective risk management requires accountability, as Cisco Systems Vice President of Governance, Risk, and Controls Philip Roush points out in the report. "If the responsible risk owner has not taken action on risks that need addressing," Roush says, "the ERM and internal audit teams inquire why this is the case and highlight the status to senior management and the audit committee as appropriate."

Achieving optimal risk management is not an overnight occurrence, as HCA Senior Vice President, Internal Audit and Risk Management Services Joe Steakley explains. His team surveys CEOs, COOs, CFOs, and chief nursing officers at approximately 170 hospitals to determine the top-ranked risks. All participants are asked identical questions. The first few years HCA conducted its risk-ranking exercise, it was clear that there wasn't a common understanding of the risks. Hospital personnel were not ranking or identifying the risks the same as corporate management and the board. Now — a decade into the process — there is a deeper understanding, a broader awareness, and the same risks rise to the surface in most interviews. "The last several years the responses have been very well aligned," Steakley says. "Last year, in fact, the board was even aligned with what the hospital staffs were saying. I believe this is a real testament to the maturity of our process."

Risk-ranking Survey

- What are the three business risks, in priority order, the company faces over the next two years that could have a significant adverse effect on the company's ability to achieve its strategic and/or financial objectives?
- What are some of the things the company is doing to help manage/mitigate each of these risks?
- In your opinion, are these risk mitigation strategies effective?

SOURCE: HCA

The IIA and RIMS agree that the better risks are assessed and managed, the better an organization is positioned to achieve its objectives. They have found that cooperation between the risk-related disciplines of internal auditing and risk management can lead to stronger practices in meeting stakeholder expectations. Specifically, the case studies featured in the report indicate that internal audit and risk management functions make a powerful team when they collaborate and leverage each other's resources, expertise, knowledge, and experience to build effective risk management processes and programs. As Philip Roush of Cisco Systems points out, "Working closely together multiplies the capabilities."

The Institute of Internal Auditors | TONE at the TOP

NONPROFIT ORGANIZATION
U.S. POSTAGE
PAID
THE INSTITUTE OF
INTERNAL AUDITORS

247 Maitland Ave.
Altamonte Springs, FL 32701-4201 USA

About *Tone at the Top*

Tone at the Top provides executive management, boards of directors, and audit committees with concise, leading-edge information on issues such as ethics, internal control, governance, and the changing role of internal auditing. It delivers relevant and timely guidance regarding the role and responsibilities for internal auditing. Email your comments about *Tone at the Top* to PR@theiia.org or call +1-407-937-1247.

About The IIA

With more than 175,000 members in 165 countries, The Institute of Internal Auditors is internationally recognized as the global voice and standard-setting body for the internal audit profession. www.globaliia.org

Complimentary Subscriptions

You, your colleagues, and your audit committee and board members receive complimentary subscriptions to *Tone at the Top*. Visit **www.globaliia.org/Tone-at-the-Top** or call +1-407-937-1111.

New Look! More Issues!

For the past two decades, *Tone at the Top* has been exploring a wide range of risk, control, and governance matters facing governing bodies and internal auditors. During that time, the world and the internal audit profession have changed a lot — and we're changing, too. We're excited to unveil a new look for *Tone at the Top*, as well as an increased distribution frequency. Instead of our quarterly publication, you can now look forward to reading new issues every other month. To view our online archive, visit: **www.globaliia.org/Tone-at-the-Top**.

6/120795/PM/BT