CFO

Governance | October 22, 2012 | CFO.com | US

Risk Management, Internal Audit Should Kiss and Make Up

Collaboration of risk-management and internal-audit functions is helping organizations improve efficiency, decision-making, and results.

Kristina Narvaez, John Bugalla

Amid the current corporate drive to cut costs and drive efficiency, insurance-related risk management and internal audit can well be seen as natural enemies, fighting for a diminishing piece of the pie. Both, after all, can lay overlapping claims to risk control, risk finance, data security, fraud prevention, and other components of what's called enterprise-risk management. A CFO or chief risk officer looking down from the top of the ERM pyramid, where the risk of an entire enterprise can be seen in an integrated way, might well feel that the potential struggle between the two functions is an inherent flaw in the process. Nevertheless, while internal audit and risk management do have different and distinctive roles regarding the ERM process, bringing them together can benefit their company.

First, it's a good idea to clearly define the correct scope of the two functions. Risk management's approach to ERM includes accountability for risk management, implementing risk responses on management's behalf, selecting the appropriate risk responses, managing assurance of risk, imposing risk-management processes, and setting the company's risk-appetite and risk-tolerance levels. The risk manager also provides processes to manage unwanted changes in expectations of the corporate strategy.

Internal audit's role includes assurance of the risk-management processes themselves, making sure the risks are correctly evaluated, determining the effectiveness of the ERM process, and evaluating and reporting key risks and reviewing the management process of such risks. Internal

audit is also typically charged with providing objective assurance to the board on the effectiveness of an organization's ERM activities. That's to ensure that key business risks are being managed appropriately and that the system of internal controls is operating effectively.

In the past, there has been some confusion about the roles and responsibilities that internal audit and risk management play in the ERM process. Who should lead the ERM effort? What are their distinctive roles in the ERM program? How can the two groups collaborate together in the ERM process?

Because internal audit and risk management are now being asked by their company executives and boards to team up to boost the value of their efforts, it's in their best interest to find ways to do so. As a result, the two disciplines at some organizations have started to share risk information to increase the awareness of the critical risks and the management and control of those risks.

By creating a dialogue between internal audit and risk management about the risks facing the organization, both groups can better:

• Identify the most appropriate ways to mitigate the risks;

• Eliminate redundancies in identifying and assessing critical risks; and

• Align their views of the organization's risk profile.

Both the Institute of Internal Auditors and the Risk and Insurance Management Society say they believe that collaboration between internal-audit and risk-management functions can lead to a stronger risk practice and better meet the expectations of internal and external stakeholders. In their combined report, "Risk Management and Internal Audit: Forging a Collaborative Alliance,"they note that these alliances have helped organizations discover efficiencies, better decision-making, and improved results.

The report discusses four case studies: Cisco Systems, Hospital Corporation of America, TD Ameritrade, and Whirlpool Corp., and how they have successfully developed open communication between internal audit and risk management. This was done by linking the audit plan and the enterprise-risk assessment; sharing available resources wherever and whenever possible; cross-leveraging each function's respective competencies, roles, and responsibilities; and assessing and monitoring their strategic risks.

For example, Cisco Systems has become adept at identifying and mitigating cross-functional risks from the input of both the internal audit and the ERM staff. Through Cisco's Risk and Resiliency Operating Committee (RROC), it has been able to determine which issues have critical risks associated with them.

Once the critical risks have been identified, the RROC constitutes a working group comprised of staff that can best address the issue in question and develop a plan to resolve the problem. The RROC's goal is to collect risk information from both the internal audit and the ERM staff to develop a series of playbooks of potential risk scenarios to help the organization know how to response to a potential risk event. Through this process, both internal audit and the ERM staff have a better understanding of the impact of the critical risks on the organization and can better evaluate how a potential risk event could be either a disruption or a competitive advantage.

Whirlpool has found that collaboration between the internal audit team and ERM staff has led specifically to consideration of how the company's critical risks are affecting their internal-control environment, and it is then able to tailor the internal-audit process accordingly. One benefit from this collaboration is the ability to share process and business knowledge to assess how risks are changing and being able to have an open dialogue on how to best optimize and leverage their combined efforts to assist the supply chain, procurement, and other business functions.

At Whirlpool, major ERM risks identified through the interview process are then rated, ranked, and assigned to one of five categories: enterprise, strategic, operational, financial, or compliance. A risk owner is identified for each critical risk that could affect the organization and given the responsibility to determine the proper risk-mitigation strategy.

This information is then shared with senior-management team and presented to the audit committee and the board as needed. The process continues with the ERM team spending a significant amount of time with executives discussing the respective risks and even more time working with their direct reports to identify projects and actions to achieve mitigation goals and objectives.

Other organizations, including JP Morgan, General Electric, and General Motors, have stated in their board-level audit-committee and risk-committee charters that the two committees will complement and collaborate, but not compete with each other. Distinct differences in the purpose, duties, and responsibilities statements of both audit-committee charters and risk-

committee charters outline that the role of internal audit is to monitor risks and risk management is to manage those risks in relationship to the organizations' strategic goals.

While there are still many *Fortune* 500 companies that have not adopted a board-level risk committee, most of those that have, have done so according to recommendations under Section 165 of the Dodd-Frank law. This section requires companies with more than $10 billion in assets to set up a risk committee responsible for oversight of ERM within the company.

For ERM to be successful in an organization, there needs to be a collaborative effort of sharing risk information generated by the internal-audit and risk-management staff not only with senior executives but also with board-level audit and risk committees.

John Bugalla is a principal with ermINSIGHTS and Kristina Narvaez is president and CEO of ERM Strategies LLC.