August 19, 2010

Internal Audit's Role in Risk Management

By Amy Borun, MBA
Partner of Candela Solutions LLC

Are you leveraging the expertise of your Internal Audit department effectively to address risk management in your company? Does your Board of Directors use your internal audit function beyond its role of testing financial reporting controls through its Audit Committee? The Institute of Internal Auditors (IIA) defines internal audit activity as:

> ***"A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes."***

If you believe that Internal Audit's role is finished once the financial audit is complete and the only recent growth in this department occurred when Sarbanes-Oxley entered the building, you are likely missing an opportunity to add value. A great opportunity exists to utilize the internal audit function to increase efficiencies and upgrade a company's risk management program. Countless articles have been written recently about the need for better risk identification and mitigation by management, as well as increased oversight at the Board level in companies of all sizes. Many of them discuss the need for greater government regulation to discourage companies from taking on more risk than they can afford. But how are these risk decisions made? What frameworks and what data are used to make informed decisions? What methods are employed to monitor and identify new, emerging risks across business functions as a company operates? Your Internal Audit department should play a key part in this research, information flow and process monitoring.

In PricewaterhouseCoopers' (PwC) 2010 "*State of the Internal Audit Profession Study*," they found that executives and Board members recognize their need to be better informed about risk management. In addition, internal auditors realize there is room to expand their role in the company. So there is a general feeling that the internal audit function could and should deliver more value. However, many companies are unsure as to what that is or how they should accomplish it. A major challenge facing these groups is in "building consensus for Internal Audit's expanded role and then delivering upon those higher expectations" according to the PwC Study. In other words, internal audit teams should re-assess their skill set and present a proposal to the Board and/or committees they report to, to facilitate better decision-making and assessment of management functions. In turn, the Board and management needs to open the way for this deeper relationship with Internal Audit and communicate what is needed for this important assurance role.

How is Internal Audit ideally suitable to advise management and directors in risk management? Under the leadership of a Chief Audit Executive (CAE), the internal audit team can apply its expertise in risk management through:

- Standards (*International Standards for the Professional Practice of Internal Auditing* created by the Institute of Internal Auditors –" IIA") set forth mandatory guidance for the professional practice of internal auditing. Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input.
- The IIA's *Assessing the Adequacy of Risk Management Processes* (PA 2120-1). This practice advisory states that "*The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes*." Practice advisories of the IIA provides strongly recommended guidance to assist internal auditors in applying the definition of internal auditing, the code of ethics, and the standards in promoting good practices. Practice Advisories address internal auditing's approach, methodologies, and consideration, but not detail processes or procedures.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management - Integrated Framework* is a detailed framework which can be used by internal auditors to analyze a risk model.
- The unique role of Internal Audit in a company typically is granted access across operating and functional areas, thus in prime position to formulate a more complete picture on the health of the entire organization. This combined with an independently organized internal audit function along with the objectivity of individual auditors should lead to more trustworthy communication with both management and directors.

Once an organization has opened the door for Internal Audit to expand its role in the risk management process, goals must be set and lines of communication must be made clear. It is important to formalize objectives and job responsibilities in writing to best enable a clear chart of information flow. First outline the set of responsibilities for each level in the organization, such as:

Board Level

- Sets the tone of the organization through management and therefore the risk appetite of the organization.
- Must communicate this tone both clearly and consistently with management, and consciously lead by example.
- While the responsibility will be for management to carry out policies, the Board is ultimately responsible to monitor the company's risk management and investigate items of concern.
- Must receive proper training to understand the business entity and the risks which face the company, and should actively seek this training from management and from outside sources.
- Should make sure lines of communication are open for all levels of staff to participate in risk management.
- Must decide what committee within its own structure is responsible for the risk management program details. It can reside in the audit committee or a stand-alone committee. Either route should have a written set of communication protocol for Internal Audit to report their findings in an independent and unbiased atmosphere.
- Should have self assessments to gauge whether its tone at the top is not only set and communicated and carried throughout the organization's actions, but also whether the tone and policies suffer from confusing "double standards." These assessments should ideally be

performed by an outside facilitator and advisor to help ensure a truly independent read on the environment.

- Should utilize the independent nature of the Internal Audit function in an advisory role for risk management training and Board self-assessments.

Management

- Must communicate the tone expected by the Board and "live the company tone" themselves. Leading by example is critical! Procedures must tie into policies set by the Board.
- Should work with the Board and Internal Audit to create a risk management program and assess its progress and report to the Board on progress and flagged items.
- Should understand the lines of communication between Internal Audit and the Board to ensure clarity.
- Should assist in training for the Board to understand the company and the challenges it faces.

Internal Audit

- Must have a clear sense of its responsibilities in risk management assurance and receive a written overview of the Board's expectations. This can be done in conjunction with a proposal from Internal Audit outlining how the department can help the Board in its work.
- With the tone expectation set at the Board level, and action plans created by management, Internal Audit can provide consultation as management creates a risk management program by performing research and ensuring adherence to a framework. As it is important for Internal Audit to remain independent without conflict of interest, the department can provide this consultation on the front end, but should not participate in administering the plan. A clear segregation of duties should be followed to help ensure independence and objectivity for eventual assurance services.
- Can run assessments of the risk management program and report to management, with emphasis on reporting both red flags and "yellow" flags which should be reported to the Board as part of their assurance services.
- Can help management train Board members regarding their fiduciary duties and risk management responsibilities.
- Can assist as an objective team member in the Board's self assessment of its own performance.

While internal audit functions have often been credited for guiding organizations through the complexities of Sarbanes Oxley and are a key player during annual financial audit cycles, many teams do not participate enough in a company's on-going risk management program. As PwCs' interviews with top executives shows - Board members, executives and internal audit teams recognize the value of a more engaged Internal Audit department, but more organizations should employ this resource. This will require better communication between these groups to understand their needs, abilities and opportunities to collaborate. With increased availability of frameworks and techniques, Internal Audit is ideally positioned to assume this extra role. A well crafted team of independent auditors is well-suited to provide fresh insights into the risks that emanate from, and have a negative impact on, business activities. However it does not happen on its own as decisions, information flows and scopes need to be defined.

*****

Amy Borun is a Partner with Candela Solutions. She manages internal assurance projects and leads our Corporate Responsibility practice and can be reached at aborun@CandelaSolutions.com.

Candela Solutions LLC is a strategic CPA firm in providing services to US public companies that external auditors cannot due to independence concerns. Visit our website at www.CandelaSolutions.com

This is an article reprint from the Governance Issues™ Newsletter, Volume 2010, Number 4, published on August 19, 2010