2007 Esther R. Sawyer Scholarship Essay

Internal Auditing and ERM: Fitting in and Adding Value

Prepared by:
John Hall
The University of Texas at Dallas

Award Topic:

Enterprise risks include both internal and external factors that can have a significant impact on organizational performance. What can the internal audit profession and individual internal audit departments do to speed up the process of integrating risk assessment methodology within the framework of the corporate governance and internal control structure?

Introduction

A recent study commissioned by the IIA Research Foundation found that 80% of respondents surveyed from the IIA's Global Auditing Information Network (GAIN) were in some stage of interaction with the Enterprise Risk Management process (Gramling & Myers 2006). If there were ever a hot topic in internal auditing, Enterprise Risk Management (ERM) is it. Senior leadership and Directors for organizations of all sizes, and from across the world are talking about ERM and how to make it work for them. This new-found interest in abandoning traditional risk management and embracing an enterprise-wide risk management approach has naturally led to several questions regarding who are supposed to be the architects, implementers, managers and overseers of the entire process. Internal audit's use of a risk-based approach easily lends itself to an interest in the ERM process, but there is considerable debate as to the role of the internal audit function in ERM (Beasley 2004). This paper seeks to define several areas in which the internal audit profession and individual internal audit departments can operate to speed up the process of integrating risk assessment methodology within the framework of the corporate governance and internal control structure while abiding with professional standards.

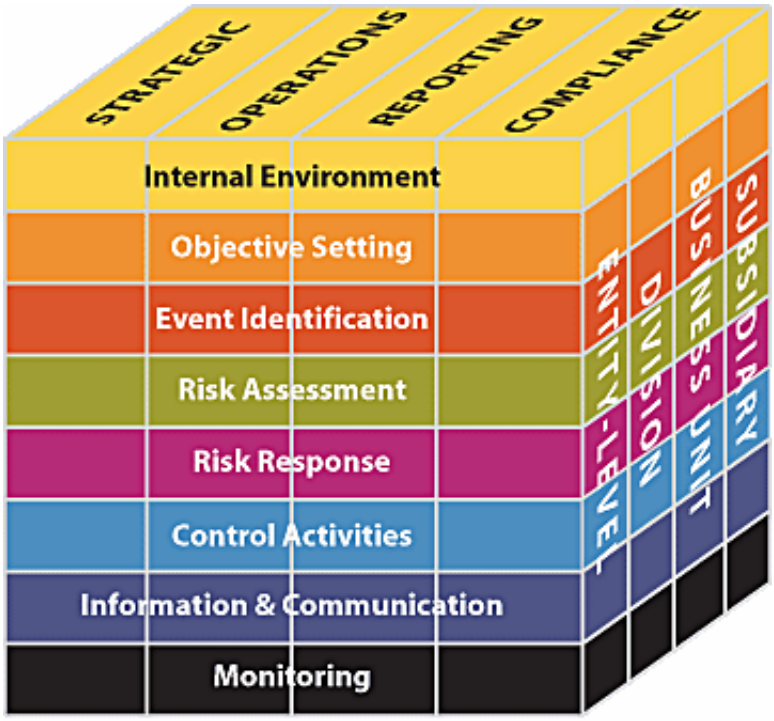
Background

It is important to establish a frame of reference, and provide some background information and definitions before internal audit's role in ERM can be expanded. In 2004, The Committee of Sponsoring Organization's of the Treadway Commission (COSO) released its *Enterprise Risk Management – Integrated Framework* and defined ERM as:

> *[A] process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*(COSO 2004).

The difference between ERM and more traditional ways of managing risks is in how the entity centralizes risk management. ERM calls for high-level oversight of the company's entire risk portfolio, rather than having many different individual managers overseeing specific risks in isolation (e.g., the "silo" or "stove pipe" approach) (Banham 2004). COSO illustrated the new ERM framework in a graphic that was similar to their well-known 1992 illustration on *Internal Control-Integrated Framework*. The ERM Framework now incorporates the Internal Control Framework and can be used to satisfy companies' internal control needs and move them to a fuller risk management process. Figure 1 depicts the COSO ERM Framework.

Figure 1: COSO ERM Framework



Across the top of the framework, the vertical columns depict the four categories that make up an organization's objectives. The horizontal rows depict the eight interrelated components of ERM, and an entity's business structures are listed down the side of the cube. The graphic portrays the ability to concentrate on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit, or any subset thereof (COSO 2004).

Figure 2, a graphic created by the public accounting firm KPMG LLP., further breaks down the differences between traditional risk management and ERM and provides a clear picture of the fundamental differences between the two risk management approaches. From the graphic, it is evident that traditional risk management is not really management at all; rather, it is, for the most part, a system of continuously and reactively dealing with risks. ERM examines risk in a new light. Under ERM, organizations view risk as something that can be planned for, oftentimes quantified, managed strategically, and ultimately leveraged against competitors.

FIGURE 2: RM vs. ERM

Traditional RM vs. ERM: Essential Differences

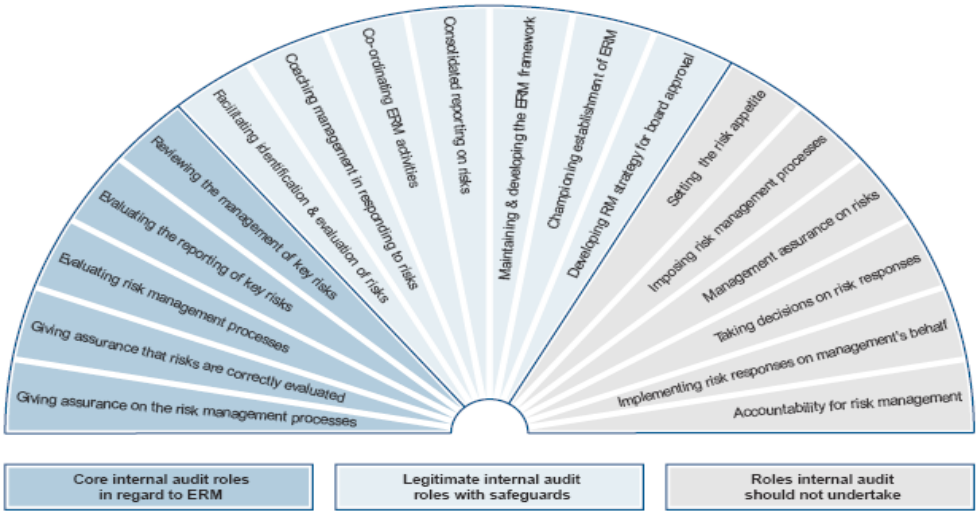
Traditional risk management	ERM
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risks with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measuring of risks
"Risk is not my responsibility"	"Risk is everyone's responsibility"

Source: KPMG LLP.

Following COSO's release of the ERM Framework, a serious debate began regarding the true role internal audit could and should play in the entire risk management process. The COSO Framework directed internal auditors to "assist management and the board of directors or audit committee by examining, evaluating, reporting on, and recommending improvements to the adequacy and effectiveness of the entity's enterprise risk management" (COSO 2004). This shift in internal audit's stated roles in the risk management function from a traditional monitoring and assurance role, to one of consulting and general oversight of the entire process was not wholeheartedly embraced and was often not fully understood. Many organizations went to either extreme in their use of internal auditing in their risk management approach. Some organizations began to have internal audit departments assume ownership over business risks while others restrained internal auditors to a strict monitoring role.

On September 29th, 2004 the IIA, in co-ordination with its IIA- UK and Ireland affiliates, released the position paper "The Role of Internal Auditing in Enterprise-wide Risk Management" in response to the release of the COSO framework. The paper suggested ways for internal auditors to maintain the objectivity and independence required by the IIA's professional standards while providing assurance and consulting services (IIA 2004). The paper designates the roles that the internal audit function should and should not be involved in throughout the ERM process. The paper achieved this by defining eighteen activities performed in the ERM process and dividing them into three key areas: core internal audit roles in regard to ERM, legitimate internal audit roles with safeguards, and roles internal audit should not undertake. The IIA has organized this information into a graphic that is often referred to as the 'ERM Fan.' (See figure 3)

Figure 3: Internal audit role in ERM



When using this graphic for direction in determining internal audit's contributions to ERM, some key factors to take into account are whether the activity raises any threats to the internal audit function's independence and objectivity and whether it is likely to improve the organization's risk management, control and governance processes (IIA 2004). The activities on the left side of figure 3 are assurance activities that an internal audit function operating in accordance with the *International Standards for the Professional Practice of Internal Auditing* can and should perform. The middle section of figure 3 illustrates the consulting roles that internal audit may assume in ERM with safeguards in place. Activities further to the right in the figure generally require greater safeguards to be in place when internal audit is engaged so independence and objectivity are maintained. Internal audit will probably not be prepared to engage in consulting activities listed in the middle section if the risk-based assurance functions in the left section of the figure are not in place first.

In evaluating the compatibility of the consulting and assurance functions, it is paramount to determine whether the internal auditor is taking on a management role. "In the case of ERM, internal audit can provide consulting services so long as it has no role in actually managing risks – that is management's responsibility – and so long as senior management actively endorses and supports ERM" (IIA 2004). On the far right of figure 3 there are six activities that the IIA has outlined as roles internal audit should not take on. These roles, if assumed with regard to ERM, could severely compromise the independence and objectivity requirements set forth in the Professional Standards. These activities are the responsibility of management and internal auditors should actively avoid involvement in them. Building off of the IIA's Position Paper, this paper will expand on a few of the key activities that internal audit departments can engage in to accelerate the implementation of risk assessment methodology into the corporate governance framework.

Internal Audit as a Catalyst

Due to their co-dependant relationship, it is not entirely fair to say that the consulting activities in the ERM fan are more important than the assurance activities in the fan. However, the consulting activities provide internal audit with the greatest opportunity to add value to the process. As such, these consulting activities represent the majority of the roles internal audit can assume in an effort to speed up the process of implementation of risk assessment methodology into the corporate governance framework.

Championing the Establishment of ERM

First and foremost, an essential activity that internal audit can engage in to speed up implementation of risk assessment methodology is championing the establishment of ERM. Phillip Fretwell, Managing Director for Protiviti Inc., presented on this subject in the September 2006 IIA Webcast. He outlined three key activities that internal audit departments can engage in to support this championing role. They were: encouraging leadership from the top, assisting in the development of a business case for ERM, and suggesting an ERM organizational structure.

Gathering support at the very top of the organization is the cornerstone of implementing a successful ERM program. This support is essential because of the very nature of the work involved in implementing ERM. Implementing ERM within an organization is not a cookie-cutter process and is often very hard and time-consuming work (IIA 2006). With a lack of demand calling for an ERM process coming from the top and no accountability for meeting project deadlines and goals in place, the project is often pushed aside when the project reaches its most difficult. People begin seeking easier projects that that senior management actually demands and has an interest in. Internal audit's close relationship with executive and senior management and the audit committee makes it very easy for them to push ERM to the forefront and gather their support.

Deloris Pettis, Director of Risk Management and Audit Services at Harvard University, spoke to this activity during the September 2006 IIA Webcast when she outlined how she and her staff went about setting Harvard's tone at the top. Their approach was multi pronged, and began with a sustained effort for several months to raise risk awareness among senior and middle management and establish a business case for ERM. This was followed by the creation of a risk management committee that was supported by senior university officials, the audit committee, and chaired by the general counsel's office (IIA 2006). This education and organization effort ignited a tone at the top for risk awareness and management at Harvard.

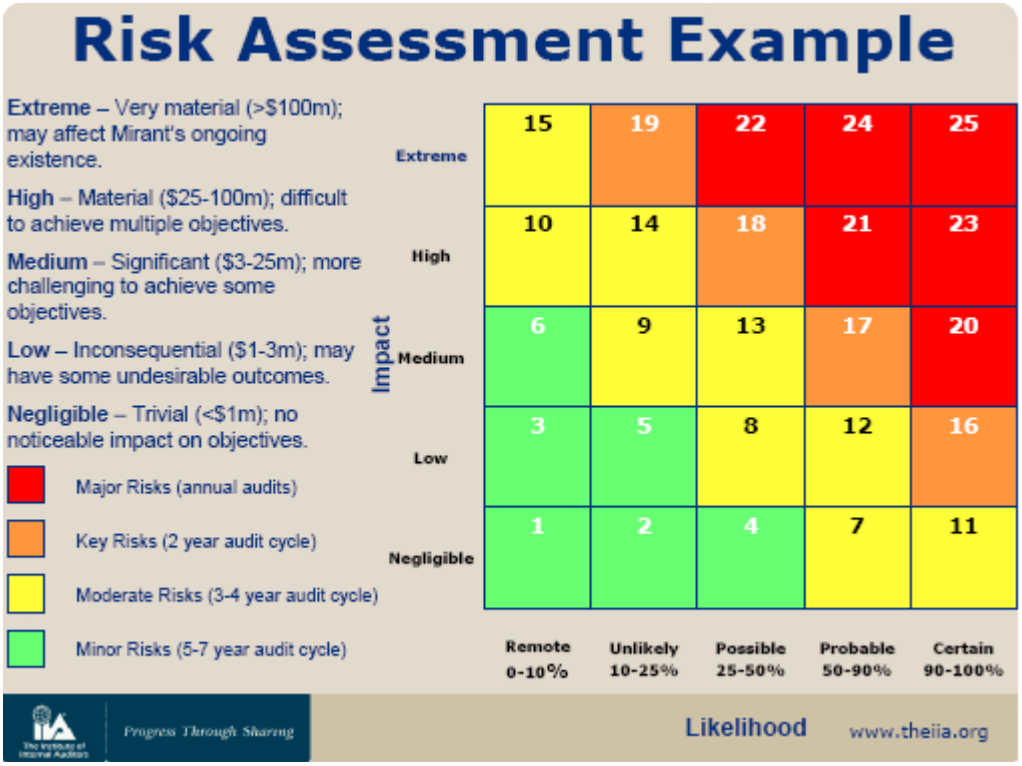
Assisting in the establishment of a business case for ERM is also an integral part to successfully championing ERM. The establishment of a business case for ERM goes hand-in-hand with establishing support for ERM at the top of an organization. Executive leadership will eventually ask 'why do this at all?' and it is important for all parties involved to understand the true value of what they are doing. Deloris Pettis accomplished this at Harvard by outlining the events that were occurring at other institutions and then explaining the possibility for these things to take place at Harvard. Then, she illustrated how these events would impact adherence to the university's values, a commitment to excellence and maintaining the public trust, if management were not proactive in preventing the events from taking place.

Internal audit can also play a part in championing ERM though the suggestion of an ERM organizational structure. Given internal audit's intimate knowledge of the organization and the distribution of risk throughout the organization, internal audit can add significant value in advising on the most efficient risk management structure. However, it is important for internal audit to ensure adequate safeguards are in place in the organizational structure to guarantee the internal auditors are not assuming management roles.

Facilitating Identification and Evaluation of Key Risks

While management must ultimately own the creation of the enterprise risk assessment, leveraging off of internal audit's annual risk assessment often provides a great framework for management to start from (IIA 2006). Internal audit could add significant value and expedite the process of implementing risk assessment methodology by leveraging their experience in developing risk assessments by assisting management in the development of an enterprise-wide risk assessment. There are a variety of risk assessment methodologies in existence and there is not a definitive format to follow. Attributes of good risk assessments are: conciseness, consistency of terminology, formal structure in the risk rating system, and general clarity of message.

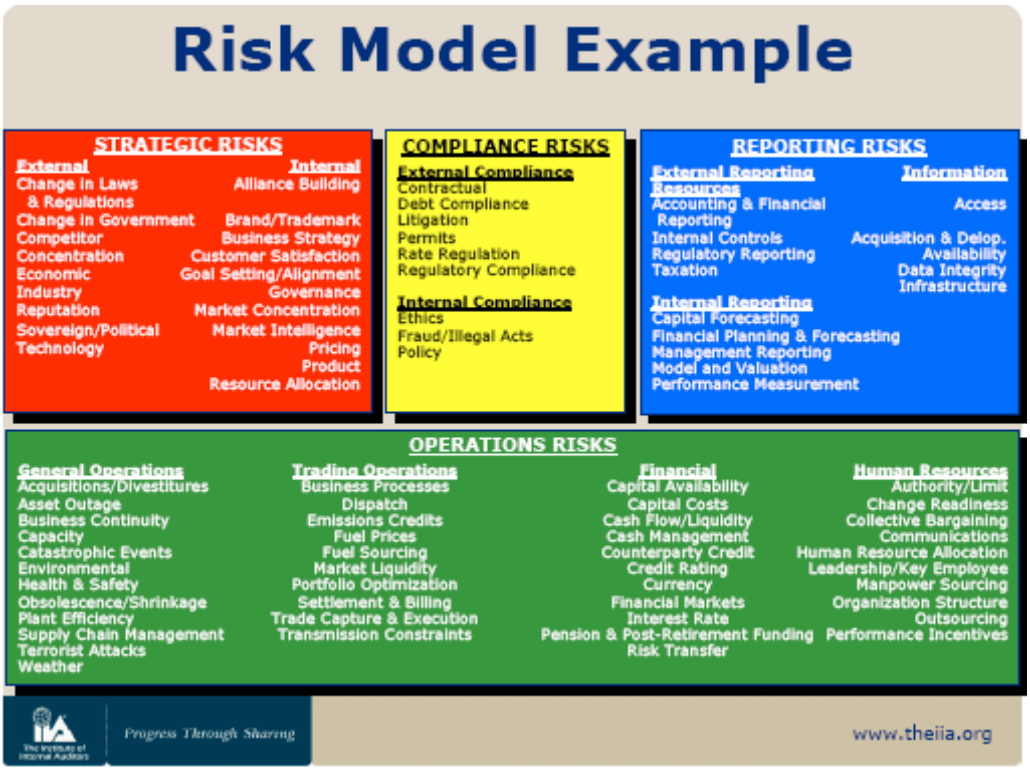
Figure 4: Risk Assessment Example



Paul Sobel, Vice President of Internal Audit at Mirant Corporation, provided figure 4 in the September 2006 IIA Webcast. This risk assessment encompasses all of the characteristics of a solid risk assessment in that it is straightforward, easy to understand, and very objective in its classifications. This would be an excellent comprehensive risk assessment framework for internal audit to provide to management for use in their development of an enterprise-wide risk assessment. However, management must be responsible for setting the risk thresholds and evaluating the likelihood of events because those ratings correspond directly with setting the risk appetite.

Internal audit could also assist in the creation of the overall risk model for the organization. Internal auditors have a unique talent in their ability to assimilate large amounts of information and organize it in a way that makes it easy for many people to understand. In the September 2006 IIA Webcast Paul Sobel illustrated an example of a risk model that shows how internal audit could be instrumental in organizing the company's risks into a COSO ERM focused risk model. In Figure 5 the risks are organized within the four main risk categories that are represented by the vertical columns in the COSO ERM cube. In each of these categories there are also sub-categories that further define the risks and help organize them.

Figure 5: Risk Model Example



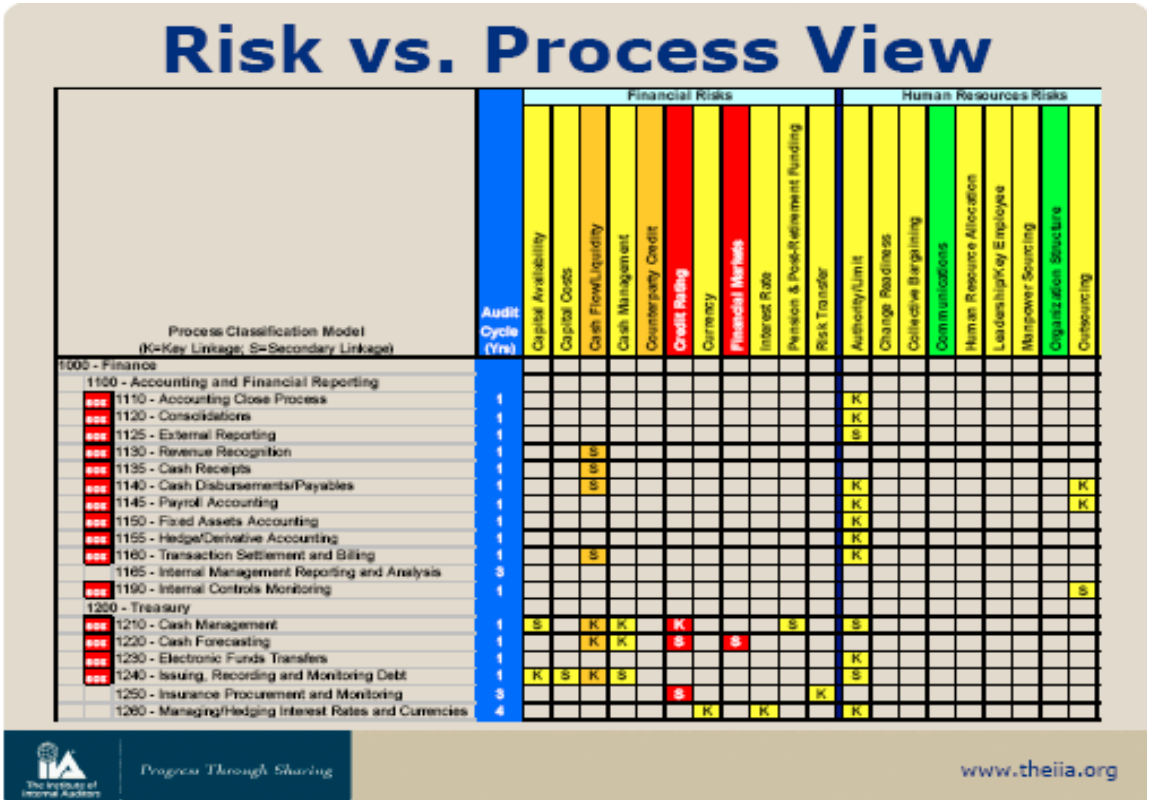
This style of risk modeling makes the information much easier to interpret and reinforces the COSO ERM framework to those who may not be as familiar with it as senior management and internal audit.

Review Management of Key Risks

While this is an assurance-based activity, internal audit's execution of this activity is essential for the implementation of risk assessment methodology into corporate governance and the internal control structure. Internal audit should go beyond traditional risk based auditing to risk management based auditing. This method of auditing closely aligns with ERM activities and the COSO ERM framework. Risk management based auditing ensures there is an understanding and alignment with business objectives and not just business risks. In addition, risk management based auditing evaluates the maturity of the risk management activity and gives consideration to management's risk appetite in reporting. This type of auditing covers all business objectives and subsequently aligns nicely with ERM (IIA 2006). In the September 2006 IIA Webcast Paul Sobel outlined three ways internal audit departments could execute risk management based audit objectives.

The first activity is targeting risks as opposed to processes in auditing. In the figure 6, the top fields are the risks that have been color coded from the risk assessment. These risks are grouped into the categories brought over from the risk model. Along the left side are the auditable processes from the risk universe. Traditionally, you would look only at the process and the individual risks associated with each process (horizontal view). In risk based auditing, you look at the risks and all of the associated processes for each risk (vertical view). This approach allows you to provide assurance as to whether or not the entire business risk has been managed.

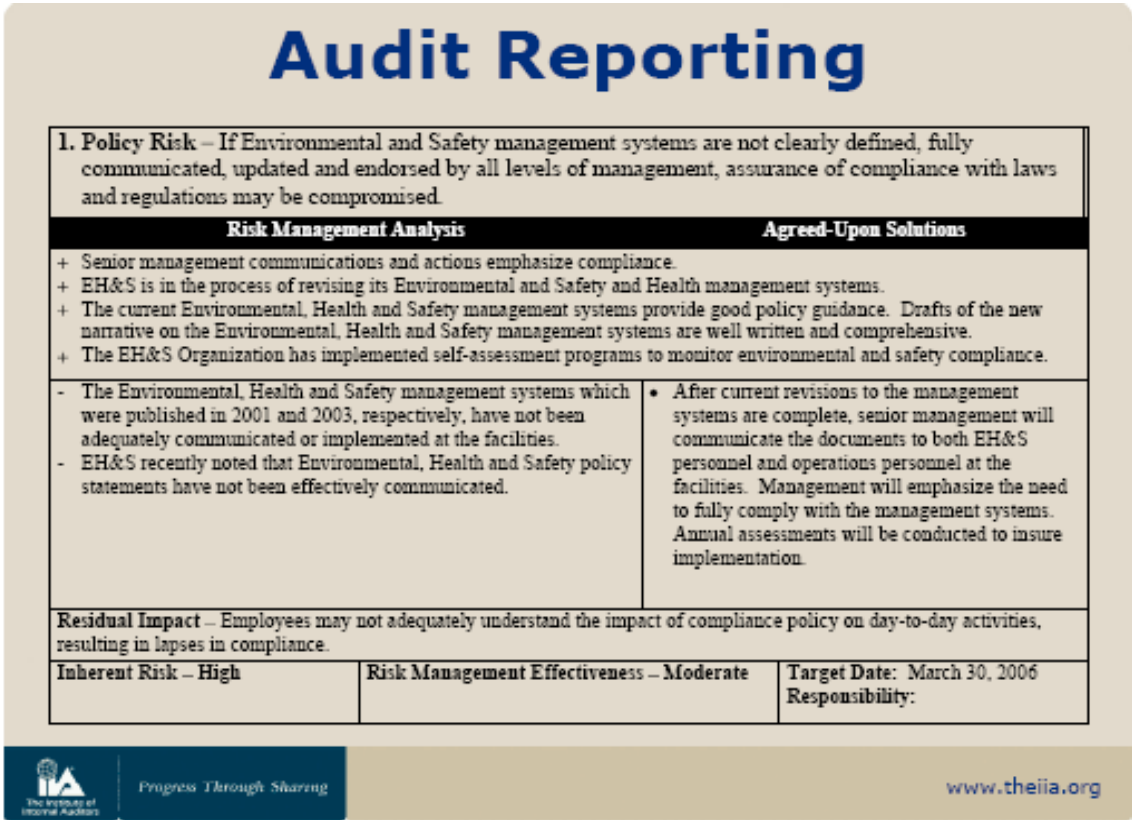
Figure 6: Risk Vs. Process View



The next activity that internal audit can perform in moving toward risk based auditing is monitoring risk management maturity. Monitoring the maturity of the risk management process provides insight on the future sustainability of risk management effectiveness. The underlying assumption is that the more mature your risk management processes are, the greater sustainability you will experience in effectively managing risks. In this sense it is a forward-looking assurance activity that closely aligns with ERM. ERM is not concerned with how well your organization managed risk in the past. It is concerned with how effectively you can manage risks going forward (IIA 2006).

The third activity that internal audit can perform in moving toward risk based auditing is concerned with audit report writing. By communicating detailed audit reports organized by risk rather than process, internal audit can emphasize the ability of the organization to effectively or ineffectively manage that entire business risk (i.e. the vertical view). In the September 2006 IIA Webcast, Paul Sobel included an example of a detailed audit report organized by business risk. In figure 7, a '+' denotes risk management activities that management is effectively deploying. A '-' denotes risk management activities that management is not effectively deploying. The residual impact statement takes the pluses and minuses into account and provides a general account of the residual risk that remains in the area. This field is important for managers as it a quick way to view a high-level assessment of your risk management efforts. The focus area in the report is the Risk Management Effectiveness rating. This area allows auditors to provide assurance on the actual management of the risk as opposed to traditional assurance on the controls for a particular business process. Issuing reports in this manner emphasizes the focus on risk management to the risk owners and further supports overall ERM goals.

Figure 7: Audit Reporting



Conclusion

Ultimately, the board and executive leadership have the overall responsibility for ensuring enterprise-wide risks are managed. Through its core assurance and safeguarded consulting roles, internal audit is well positioned to add significant value to the ERM process. Through all of its ERM activities, internal audit must apply all relevant Standards in order to protect its independence and objectivity. Within the constraints of the Professional Standards, ERM can help raise the profile and increase the effectiveness of internal audit (IIA 2004). Internal audit's intimate knowledge of an organization's risk universe, familiarity with risk-based assessments, close ties to executive leadership, and unique ability to assimilate large amounts of information and produce clear and concise findings position internal audit as a valuable instrument in an organization's ERM implementation and ongoing assurance and consulting activities.

Works Cited

Gramling, A.A., & Myers, P. (2006), "Internal Auditing's Role in ERM" *Internal Auditor* (April 2006), 52-58

Banham, R. 2004. Enterprising views of risk management. *Journal of Accountancy* 197 (6): 65-71.

Institute of Internal Auditors (IIA). 2004. *The Role of Internal Auditing in Enterprise Risk Management* (September). Altamonte Springs, FL: The Institute of Internal Auditors.

Internal Audit Standards Board (IASB). 2004. *International Standards for the Professional Practice of Internal Auditing*. Altamonte Springs, FL: Institute of Internal Auditors.

Committee of Sponsoring Organizations (COSO) (2004*), Enterprise Risk Management - Integrated Framework*, New York, COSO.

Beasley, M.S., Clune, R., & Hermanson, D.R. (2004), *Enterprise Risk Management and the Internal Audit Function*, Altamonte Springs, FL, Institute of Internal Auditors Research Foundation.

Beasley, M.S., Clune, R., & Hermanson, D.R. (2006), *The Impact of Enterprise Risk Management on the Internal Audit Function*, Altamonte Springs, FL, Institute of Internal Auditors Research Foundation.

IIA Webcast. September 19, 2006 1:00PM EST

Presenters:
Michael J. Head, CIA, CPA, CMA, CBA, CISA
Managing Director Corporate Audit
TD AMERITRADE
Paul Sobel, CIA, CPA
Vice President of Internal Audit, Mirant Corporation
Deloris Pettis, CIA, CPA
Director of Risk Management & Audit Services
Harvard University
Phillip Z. Fretwell, CPA
Managing Director
Protiviti Inc.

Sources for figures used in text

Figure 1: Committee of Sponsoring Organizations (COSO) (2004*), Enterprise Risk Management - Integrated Framework*, New York, COSO.

Figure 2: Banham, R. 2004. Enterprising views of risk management. *Journal of Accountancy* 197 (6): 65-71. (originally from KPMG LLP)

Figure 3: Institute of Internal Auditors (IIA). 2004. *The Role of Internal Auditing in Enterprise Risk Management* (September). Altamonte Springs, FL: The Institute of Internal Auditors.

Figures 4, 5, 6, & 7: IIA Webcast. September 19, 2006

