Ten steps to enterprise-wide risk management

Priscilla Burnaby and Susan Hass

Priscilla Burnaby is a Professor at Bentley College, Waltham, Massachusetts, USA. Susan Hass is a Professor at Simmons College, Boston, Massachusetts, USA.

Abstract

Purpose – *The purpose of this paper is to discuss the objectives of enterprise-wide risk management (ERM), the Committee of Sponsoring Organizations (COSO) ERM Framework, and outline a method to implement ERM in organizations.*

Design/methodology/approach – *This paper delineates ten steps organizations can use to develop a viable ERM system for any organization.*

Findings – *It is highly recommended that a high-level risk officer with visible support from senior and board level executives has a separate function to oversee the development of an ERM department.*

Practical implications – *Although the internal audit department has a large role in evaluation and monitoring the ERM system, it is management's responsibility to develop a strong ERM function that ties corporate strategy, the budget, controls, and the entity's performance measurement systems to risk management.*

Originality/value – *The cost to the entity of implementing and maintaining of an ERM system is grossly out-weighed by the results and knowledge gained in evaluating, assessing, and overseeing risk to insure achievement of strategic objectives over the short- and long-term life of the organization.*

Keywords *Risk management, Control systems, Risk assessment, Reports*

Paper type *Viewpoint*

Introduction

What impact will increased gasoline prices have on the price of plastic? Will political instability in Latin America affect the supply of raw materials in the next six months? In the next year? In the next two years? Has global warming really changed the ocean tides, and if so, will it affect the planned wind farm off the New England shoreline? Will my secret formula for our best selling chili remain safe or will hackers be able to get through our security system? If I vertically integrate, my company's value will increase but so will my exposure to external risks. These and many other economic events lead to risks that affect business on a daily basis and are part of doing business. Companies need to build risk management into their corporate strategy and daily operations. To hold risks in check, organizations must plan to protect themselves so that only an acceptable level of residual risk remains. Each company's managers decide what their risk appetite is and what the costs and benefits are for risk avoidance or risk acceptance.

The growing trend is for companies to take an enterprise-wide risk management (ERM) approach to protecting themselves against the many risks of running an organization. There is interest in accelerating the evolution of ERM as a core business process (Francis and Richards, 2007). All entities face a multitude of risks that if not identified and integrated into an overall business strategy may result in lost revenues or a business failure. Several organizations, including the US government, have made it a priority for companies to create risk and control systems that result in reliable financial reporting systems that have adequate controls. The Institute of Internal Auditors (IIA) Research Foundation has listed the study of

Received: 29 October 2007
Revised: 19 March 2008
Accepted: 5 June 2008

DOI 10.1108/14720700910998111

current practices in ERM and Performance Measurement Systems as one of its top research priorities for both operational and financial reporting. The Institute of Internal Auditors Research Foundation Sub-committee on Risk Management states that, ''many companies and organizations have recognized the need to effectively identify and manage a combination or basket of threats and exposures facing them in today's complex, global environment'' (The Institute of Internal Auditors Research Foundation, 1999).

In the USA, the Sarbanes-Oxley (SOX) Act of 2002 (Act) (Securities and Exchange Commission, 2002) requires annual reports to contain an internal control report and for the CEO and the CFO to certify to the fairness of the public reports. The Act also requires that organizations select a control framework. In 2004, the Committee of Sponsoring Organizations (COSO) created the Enterprise Risk Management Framework to provide guidance for entities in developing control systems that aid organizations in managing risk. Based on this report, The IIA (The Institute of Internal Auditors, 2004) released guidelines delineating the internal auditor's role in ERM. This role includes giving assurance on the management process for reviewing the management of key risks.

The purpose of this paper is to discuss the objectives of ERM, the COSO ERM Framework, and to outline ten steps to implement ERM in your organization.

Enterprise-wide risk management

The objectives of enterprise-wide risk management are first, to develop strategic corporate objectives that are measurable, second, to identify risks that would prevent accomplishing the corporate objectives, and, third, to identify controls that would mitigate those risks. Closely linking risk management to strategy is the hallmark of true ERM programs (Francis and Richards, 2007). Risk is anything that gets in the way of an organization achieving its' objectives. Risks are inevitable and are a function of the strategic objectives and the way an organization is run. Managers put assets at risk to achieve objectives. Risk is the uncertainty of plans and decision outcomes (McNamee and Selim, 1998). It is the anxiety of unknown future events and the negative consequences of their outcomes (Irwin, 2007). ERM includes the analysis of risks surrounding the development of performance measures, critical success factors, and efficient systems based on corporate strategy and corporate objectives to influence decision making and managerial action plans. ERM activities can be performed by a management team, department, external auditors, consultants, or internal auditors.

An example of a risk management process is the Australian Customs Service's six-step continuous improvement process at the operational and tactical risk management levels (McNamee and Selim, 1998):

1. *Risk identification*. What could go wrong, how it happens, and why it happens.
2. *Risk analysis*. Estimating the likelihood and consequences of the decision.
3. *The risk management solution*. Various mitigation treatments, including controls.
4. *Evaluation and audit*. Subsequent review of the effectiveness of the risk management solution.
5. *Performance measurement*. Review of the costs of risk mitigation.
6. *Final review*. Gleaning the lessons learned to serve as a guide for future situations.

Fidelity Investment's Risk Management Department has developed a form for each of their divisions to report on a few key performance measures based on the division's objectives that tie to corporate objectives. They also report on any losses incurred and their cause. The Risk Management Department compiles this information for upper management and the Board of Directors (Gaquin, 1999).

External auditors now begin their financial statement audits by examining the underlying business strategy and objectives of the organization to determine if the organization has controls in place that result in reliable financial information. Auditing firms offer a more in-depth risk assessment beyond the needs of the financial statement audit (Deloitte &

Touche, 1998; Coopers & Lybrand, 1998). An example of a large auditing firm adopting a process risk-based approach is KPMG's Business Measurement Process (BMP). BMP incorporates analysis of the entity's strategy in a ''top down'' risk-based process approach for a financial statement audit (Bell *et al.*, 1997).

The IIA conducted a study, *Risk Management: Changing the Internal Auditor's Paradigm* (McNamee and Selim, 1998). Their research indicated a rapid change in the internal audit process from a passive and reactive control-based auditing approach to an active and anticipative risk-based audit approach. At a time when outsourcing the internal audit function is an option for an organization, the internal audit department needs to provide services that can be shown as value-added. With their knowledge of the organization and their skills in audit, research, and analysis, internal auditors should play a key role in enterprise-wide risk management. As they have been using risk models to determine which areas to audit in an organization, internal audit departments have a great deal of experience in analyzing risk.

Ten steps to risk management

The following outlines ten steps to develop a viable ERM system for any organization. The ten steps are:

1. Mandate from the top.
2. ERM department and buy-in.
3. Decide on control framework.
4. Determine all risks.
5. Assess risks.
6. Business units objectives and performance measures.
7. Objectives and control summary.
8. Monthly ERM reporting system.
9. Analysis by ERM department.
10. Continuously monitoring the process.

It is recommended that a high-level risk officer have a separate function to oversee the development of an ERM department. Although the internal audit department can have a significant role in evaluation and monitoring the ERM system, it is management's responsibility to develop a strong ERM function that ties corporate strategy, budget, controls, and performance measurement systems to risk management.

Step 1. Mandate from the top

In order for a formal and documented ERM process to work, it must be mandated by the board of directors (Board), chief executive officers, and other top level management of the organization. Because business is risk management, understanding the risks accepted by the company as it pursues its strategy to achieve its objectives is essential for the board and relevant stakeholders (King, 2001). Risk management is central to the execution of the organization's strategy so there must be a linkage between the organization's strategic plan and initiatives and an understanding of all organizational risks across the entity. The coordination of risk assessment and strategy development will assure that both internal and external stakeholders will consistently manage organizational risk effectively and efficiently. A mandate from the top is needed to assure the risk management team's success in establishing the ERM program to aid in the achievement of organizational goals.

To understand the financial commitment the process will take, the Board should oversee a study to estimate the cost to implement an ERM department. Once the costs are understood, it may be best to hire an expert consulting team to provide technical assistance to management in the development of an implementation plan and to designate an internal team to be responsible for the implementation. To be successful over time, a separate department for ERM should be empowered to collect risk reports monthly and assimilate information to be reviewed by the Board. At a minimum for smaller organizations, there should be a chief risk officer assigned to monitor the process.

Step 2. ERM department and buy-in

There should be several layers of ownership for the ERM process. A senior level manager must be responsible for development of the ERM Department and role-out process. This is the ERM champion who will determine the appropriate levels of resources and time commitment needed. A team of senior managers must drive assessment, evaluation, and development of an action plan. They will develop the time table for implementation and educational programs, hold meetings with each area to develop risk report requirements, and create a procedure manual for all participants.

Execution of the ERM process will be implemented by a management team at all levels of the organization. A formal process with a realistic timeline must be established. All members of the organization need to participate to insure that all risks are known and that key risks are managed by department or reporting unit under a comprehensive master plan. The internal audit department cannot be responsible for risk management but can be involved in the development and monitoring of the risk management plan.

Ownership also means accountability. Individuals that oversee risk management activities in each department must be accountable for the quality of their risk reports and activities under the risk management umbrella. Having concentrated ownership ensures accountability. Well-managed organizations will also tie individual compensation and promotion to the success of risk management initiatives.

Although the mandate for risk management comes from the highest level and a senior level risk champion oversees risk management activities, employees at all levels within the organization are responsible for the success of the risk management initiative. Existing risk managers should be enlisted in this effort to help train and educate all employees about risks and risk management.

Without everyone in the organization understanding the importance of a successful risk management initiative, the company may be at risk for significant loss due to little known, but not unknown, risks. For example, a purchasing agent may know of anticipated limitations in the supply of a key raw material and try to manage the problem himself. He fails to report this situation in the periodic risk reporting system. When the supply of this key resource is reduced to unacceptable levels, the company, but not the employee, is taken by surprise. The company must react immediately, but does not have a contingency plan, since leadership was not aware of the problem. If the employee truly understood the nature of ERM and its import to the entity, the risk would have been included in the department's analysis and monitored with plans in place time to find an alternative source or resource with minimal interruption.

Step 3. Decide on control framework

In order for ERM to work, organizations must commit to the adoption of an internal control framework. The existence of a satisfactory internal control structure reduces the probability of errors and irregularities. In the USA, the SOX Act of 2002 (Act) (Securities and Exchange Commission, 2002) requires annual reports to contain an internal control report and for the CEO and the CFO to certify to the fairness of the public reports. In 2002, internal auditors' audit scope increased when the IIA expanded their role to include assurance services and consulting to improve the effectiveness of risk management, control, and the governance process.

As a response, in 2004 the COSO expanded their suggested control framework from five elements to eight to better address how organizations could better manage enterprise risk. The components were derived from the way management operates a business, and they should be integrated with the management process. A summary of the eight components can be found in Table I. This is one of several internal control frameworks available for use by organizations.

Step 4. Determine all risks

An effort must be made across the entity to collect all known or anticipated risks. If risks are managed in organizational silos, poor communication and the resultant ignorance of the full potential of organizational threats could result in an iceberg of risk. Known risks are reduced and the hidden ones could sink the corporate ship (Rasmussen and McClean, 2007). All employees are responsible for identifying and sharing potential organizational risks. Those that affect the achievement of the organization's strategy are most important, but this assessment will be done in a later step. Based on discussion across the organization, a Risk Dictionary should be developed so that everyone agrees on the meaning of each risk term. This Risk Dictionary will be used in all education programs to roll out the ERM program to each department or unit. This step is just a data collection and risk definition effort. Value

Table I Components of internal control

Components	*Description of component*	*Key elements*
Internal environment	Actions, policies, and procedures that reflect the overall attitude of top management, directors, and owners of an entity about control and its importance	Risk management philosophy Risk culture Board of directors Integrity and ethical values Commitment to competence Management's philosophy and operating style Risk appetite Organizational structure Assignment of authority and responsibility Human resource policies and practices
Objective setting	Precondition to event identification, risk assessment, and risk response	Strategic objectives Related objectives Selected objectives Risk appetite Risk tolerance
Event identification	Management identification of interrelationships between potential events and categorization of events	Events Factors influencing strategy and objectives Methodologies and techniques Event interdependencies Event categories Risks and opportunities
Risk assessment	Management's consideration of the extent to which potential events might have an impact on achievement of objectives	Inherent and residual risk Likelihood and impact Methodologies and technologies Correlation of events
Risk response	Management's determination on how to respond to assessed relevant risks	Identify risk responses Evaluate possible risk responses Select responses Portfolio view
Control activities	Policies and procedures that help ensure that management's risk responses are carried out	Integration with risk response Types of control activities General controls Application controls Entity specific
Information and communication	Information to be identified, captured, communicated in a form that enable personnel to carry out their responsibilities	Information Strategic and integrated systems Communication
Monitoring	A process that assesses both the presence and functioning of its components and the quality of their performance over time	Separate evaluations Ongoing evaluations

Source: Committee of Sponsoring Organizations (2004) judgments as to likelihood of an event occurring or financial impact are not to be made at this time. Based on the area's objectives, each reporting department or entity needs to provide input on the risks of not achieving the objectives. At the stage of designing the area's report, the objectives and risks will be tied to performance measures.

Includable risks must go beyond consideration of compliance, legal, and financial risks. Look at internal risks (information technology, business processes, support and documentation) and external risks (political, social, environmental, governmental and economic) (DeLoach, 2000). Many organizations currently spend significant time and money on compliance risks from laws and regulations. To limit the risk assessment to compliance related areas would seriously undermine the value of this effort.

The accumulated risk list should be very extensive. An evaluation of the risk exposures cannot be made at the business unit level that identified it initially, since the linkage of risks across the entity may indicate it is more significant than initially thought. Consider the following risk groups when accumulating the Risk Dictionary:

- strategic;
- reputation – negative public relations;
- business operations – fraud, lost revenue, unauthorized actions;
- regulatory compliance – SOX, SEC, EPA, laws at all levels;
- contractual obligations – joint ventures, vendors, third parties;
- market – external factors (economic conditions, competition); and
- human resources – quality and quantity of people.

Step 5. Assess risks

The next step is to determine risk priorities, both for the company and for the business unit by using a risk mapping technique. This process is done before considering the mitigation of risks resulting from internal controls or other risk mitigation methods such as insurance. Each risk must be evaluated for the impact of potential loss or consequence of the risk to the company. Risks are categorized by their potential impact on financial or resource loss:

- minor;
- damaging; or
- catastrophic.

Then the likelihood of the risk should be categorized as:

- unlikely;
- possible; or
- probable.

Based on this analysis, the risks are mapped in a table (see Figure 1) that classifies all the risks identified in step four (KPMG, 1999).

After consensus from key players and constituencies on the results of this effort, particular attention should be given to those risks categorized in the high impact and high likelihood categories. While much less attention is usually given to risks classified as ‘‘1’’, all identified risks should be evaluated. How each entity decides on the methods used to reduce or accept risk depends on their risk ‘‘appetite’’.

After mapping the risks, consider the existing environment, the corporate strategy, and those risks that could impede achieving stated goals and objectives. Decide what controls are in place that could mitigate the risks and what controls would be needed if they were not already in place. Assess the resultant residual risks in the context of which are necessary and must be managed. The conclusions reached should result in risks being put in the following categories (DeLoach, 2000):

Figure 1 Analysis of risk

Likelihood of Occurrence	Probable			
	Possible			
	Unlikely			
		Minor	Damaging	Catastrophic
		Impact on the Organization		

- Retain the risk and monitor it on a regular basis. For the risks the organization accepts, it can increase the price of the product to absorb the potential cost of the risk, self insure, or plan on the risk by setting up reserves.
- Reduce the risk dispersing or developing controls.
- Avoid the risk by divesting or eliminating the process that is causing the risk, and prohibit or stop the activity.
- Transfer the risk by partnering through insurance, hedging, sharing, or outsourcing.
- Exploit the risk by diversifying, expanding, creating, redesign, reorganizing or renegotiating.

Based on the analysis of risks, the ERM implementation team can work with each reporting department-level to link the organization's strategy to that area's objectives and residual risks to develop performance measures to be reported to the risk department. This will allow the organization to monitor progress on achieving the corporate objectives and highlight areas where improvements need to be made or problems need to be addressed.

Step 6 Business units objectives and performance measures

At this stage, the implementation team needs to review company strategy with each business unit to determine how the unit's deliverables result in the achievement of the corporate objectives. Department level objectives must be identified that enable the organization's strategy to be achieved. The objectives should contain defined targets and be SMART. SMART objectives are Specific, Measurable, Achievable, Results-oriented, and Timely. Based on the targets, performance measures should be developed to compare actual results to the targets. As performance measures affect behavior, they should be easily understood by all employees, achievable, limited in number, and result in the correct behavior. Unethical behavior can result if employees' have unattainable goals set for them or misunderstand the objective.

As it is impossible for a manager to manage 20 key indicators, the objectives and performance measures should be limited. To wisely utilize employees' time, indicators should be focusing only on those performance measures and targets that are critical to organizational success. Since performance measures affect employee behavior, one does not want diluted performance results because of a ''shotgun'' approach that monitors too many measures. Uunderstanding that since most measures are related, focusing only on key indicators results in achieving the desired objectives.

Step 7 Objectives and control summary

An example of a risk analysis format that could be used to communicate the results of a risk analysis process audit is shown in Table II. It is a good format for each unit to complete to decide which objectives, performance measures, and risks will be reported to the ERM Department for monthly review. This chart is completed using an example of a hotel losing its five star rating. By not having total employee understanding about the hotel's strategy and the risks that may impede its achievement, the hotel lost its five star rating because the telephone was not answered in three rings. One relatively low paid employee hurt the hotel in a critical way and damaged its ability to achieve not only its strategy but also the desired level of financial success.

This demonstrates the importance of combining the strategic objectives of the entity to the related performance measures, critical success factors, risks, and controls for the process under audit. In the USA, due to the required SOX Act of 2002 (SOX) review of internal controls by external auditors, many organizations may have much of the information needed to prepare this report. After the chart is completed, key stakeholders should meet and decide what added controls or actions must be taken. Responsibility for oversight must be assigned and a timeline for review and assessment must be established. Assigning accountability is critical in risk management.

John Hancock maintains a control system through its internal audit function that is based on the COSO framework. At the end of each audit, a control summary relating all of a function's control procedures to the business and control objectives and risks associated with that function is prepared. After the passing of SOX, the chief financial officer required all company functions to develop, prepare, and retain control summaries which are now maintained on a web-based enterprise-wide controls database. Each control summary has an officer as its owner who must quarterly assess the controls in his function (Robitaille, 2004).

Step 8 Monthly ERM report format

Having a risk management plan and implementing it is not adequate for ensuring that the plan is followed or that the company is controlling its risks. A feedback loop ensuring that the report results get back to the ERM department, upper-level management, and the Board is vital to organizational and strategic success. The reporting structure should do or include the following in a monthly monitoring system:

1. Define the specific process within the department.
2. Define the specific risks of not reaching the targets identified in the department objectives' that tie into the overall corporate objectives.

Table II Objectives and control summary

Objective and related performance measure(s)	*Performance measure*	*Critical success factor*	*Risks*	*Control strengths in the process*	*Suggestions for improvements (may increase or decrease controls)*
Telephone calls are to be picked up within three rings	Percent of time the telephone is not picked up in three rings	Enough trained staff to answer the phone	Loss of five star rating	Special ring indicating the third ring	Hourly, supervisor reviews electronic reports of the number of times telephone is not answered within three rings to determine the need for extra staff

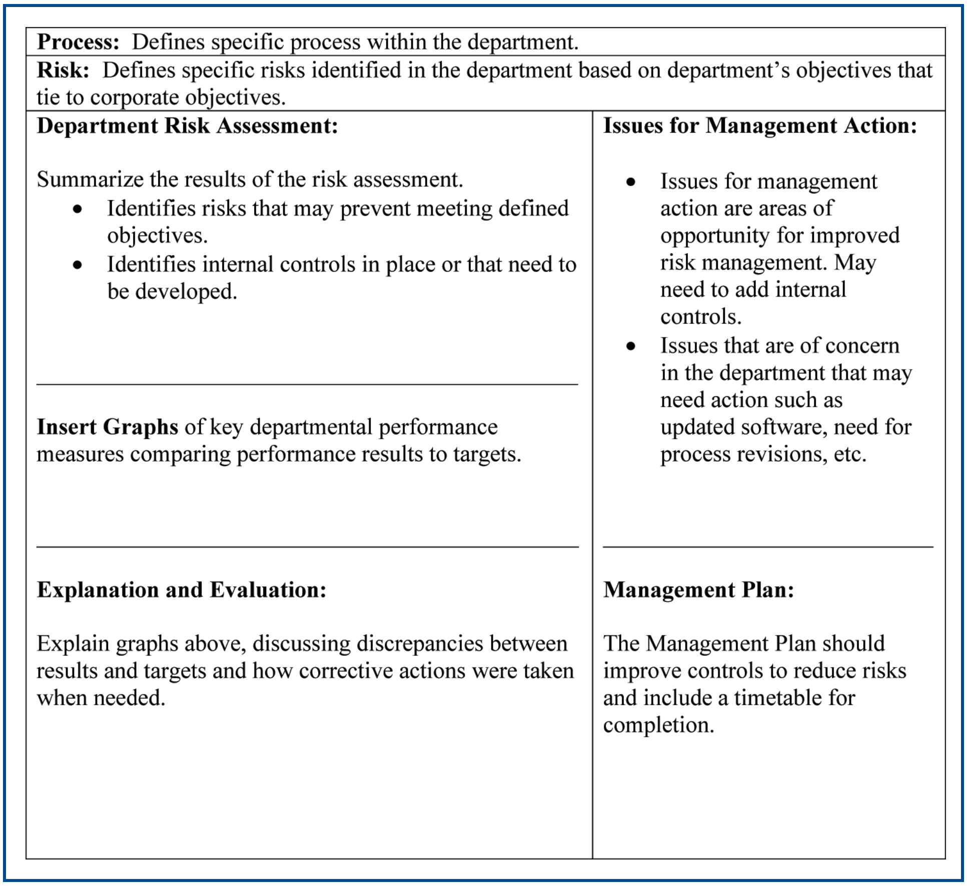
3. Summarize the results of the department's risk assessment by asking what risks could prevent meeting the identified objectives and what internal controls are in place or need to be developed to mitigate the risks.
4. Insert a performance measurement graph or specific language to show how often the target is being reached. It is critical to explain when results are in the danger zone and how they were or should be corrected.
5. Explanation and evaluation of the reported results in the graphs should be included to show how corrective actions were taken or needed.
6. Identification of issues for management action plans in areas of opportunity for improved risk management. They may indicate a need to add internal controls and issues that are of concern in the department that may need action, such as updating of software or the need for process revisions.
7. An action plan to address problems identified by the reporting system is mandatory for proper risk control. It may include the need to improve controls or the need to review the likelihood/probability assessment.

Figure 2 presents a format for a Monthly Department Risk and Performance Report that could be developed for each reporting entity.

Step 9 Analysis by ERM Department

The Monthly Department Risk and Performance Report can be used in many ways. The department issuing the report can measure progress and monitor key targets for the area's

Figure 2 Monthly department risk and performance report



Process: Defines specific process within the department.

Risk: Defines specific risks identified in the department based on department's objectives that tie to corporate objectives.

Department Risk Assessment: Summarize the results of the risk assessment. • Identifies risks that may prevent meeting defined objectives. • Identifies internal controls in place or that need to be developed.	**Issues for Management Action:** • Issues for management action are areas of opportunity for improved risk management. May need to add internal controls. • Issues that are of concern in the department that may need action such as updated software, need for process revisions, etc.
Insert Graphs of key departmental performance measures comparing performance results to targets.	
Explanation and Evaluation: Explain graphs above, discussing discrepancies between results and targets and how corrective actions were taken when needed.	**Management Plan:** The Management Plan should improve controls to reduce risks and include a timetable for completion.

contribution to realization of the organizations strategy. This process can be used to alert the area when corrective action needs to be taken. The Risk Department would summarize the information for upper management and the Board to assess progress towards achievement of overall corporate goals and to alert them of high-risk areas that need attention. The information could also be used to share best practices and alert the internal audit department about high-risk areas that may need to be reviewed for adequacy of internal controls.

Corporate governance includes implementation of a control framework and continuous improvement and monitoring of a control structure, all of which should be included in an ERM management system. As part of their corporate governance process, John Hancock requires each department manager to quarterly update their Control Summary Database (CSD) Table. The CSD Table includes the department's objectives based on corporate strategy, risks, exiting controls, and needed controls. Based on the CSD, the internal audit department evaluates the process and gives it a grade. The CSDs are available to internal and external auditors, senior management, and the audit committee of the board. Negative evaluations and outstanding control issues are reported to the Disclosure Committee consisting of the CFO, general audit director, and all senior executives. The Disclosure Committee reviews the certification results and reports its conclusions to the CEO. These reviews cover all COSO control categories, financial reporting, operating and regulatory controls. (Robitaille, 2004) This risk management process assures that all major risk and control weaknesses are discussed at the board level and that management is held accountable to make the needed control upgrades.

Step 10. Continuously monitoring the process

On a regular basis, the ERM department should do an analysis of internal and external events that could force revision of the overall strategic plan. Each unit should evaluate how these changes would affect their targets and risks. Examples of questions that need to be addressed are:

- Is senior management still actively committed and involved?
- Has the risk champion lost interest in the initiative?
- Are the risk management budget, timeline and priorities reviewed annually?
- Are people at the appropriate levels monitoring the results of the existing system ensuring display and collection of relevant information?
- Are risks properly addressed in the context of strategy and objectives annually?
- Are controls annually reviewed for their effectiveness in mitigating risks?
- Has ownership and accountability of the risk management effort changed?
- Are there changes in internal risk factors – strategy, business objectives, people, product/services, systems or processes?
- Are there changes in external risk factors – environment, competition, social, political, economic, etc.?

After answering these questions, the ERM department must make any appropriate revisions to the risk management system and related areas, ensuring that there is still entity-wide support.

Implementation

The initiatives related to this mandate should be implemented initially via a pilot test. The pilot test must be successful in order to encourage participation by other units. Participants need to see that the ERM adds value to the efficiency and effectiveness of their process and is not just adding another layer of reporting. After the success of the pilot test, the initiatives can be rolled out to more units and then throughout the company.

Select a test site that has the potential of a successful implementation of the ERM reporting. After three and six month periods, review the performance measures selected for the test site to determine if employee behavior has been positively or negatively modified and if the correct performance measures were selected. Look strategically at the effectiveness of the risk identification process, the risk management plan, the reports and reporting system, acceptance and understanding of risk management throughout the selected organization and the level of support from the top. Determine whether changes must be made in the implementation process before working with other units or incorporating risk management companywide. The strategic plan should be tied to a rolling budget and employees' performance evaluation and remuneration should be tied to how well they meet their units' targets.

During implementation, consider the importance of the unit to achievement of corporate strategy, the perceived or actual risk to the company, the compliance environment, the location and size of the unit, and the ability to staff the ERM process appropriately. Consideration must be given to these areas as successful implementation at the local level contributes to the success of the strategy at the company level.

Conclusion

Managing risk is part of corporate governance and the ability of an entity to strategically achieve results. The ten steps listed above are a general framework that allows organizations to identify, control, and manage risks that could impede its ability to achieve their desired operating results. The cost to the entity of an ERM system is grossly out-weighed by the results and knowledge gained in evaluating, assessing, and overseeing risk to insure satisfactory achievement of identifies strategic goals over the short- and long-term life of the organization.

References

Bell, T., Marrs, F. and Thomas, H. (1997), *Auditing Organizations Through a Strategic-Systems Lens The KPMG Business Measurement Process*, KPMG Peat Marwick LLP, Minneapolis, MN.

Committee of Sponsoring Organizations (2004), Enterprise Risk Management Framework.

Coopers & Lybrand (1998), ''Operational financial and compliance risk: are you in control?'', *Presentation*, 12 May.

DeLoach, J. (2000), *An Executive Summary of Enterprise-wide Risk Management Strategies for Linking Risks and Opportunity*, Arthur Anderson, Chicago, IL.

Deloitte & Touche (1998), *Enterprise Risk Services*, Deloitte & Touche LLP, New York, NY.

Francis, S. and Richards, T. (2007), ''Why ERM matters ... and how to accelerate progress'', *Risk Management*, 15 October, pp. 28-31.

Gaquin, M. (1999), ''Firmwide risk management, fidelity investments'', class presentation, 6 October 1999.

(The) Institute of Internal Auditors (2004), *The Role of Internal Auditing in Enterprise-wide Risk Management, Position Statement*, The Institute of Internal Auditors, Altamonte Springs, FL.

(The) Institute of Internal Auditors Research Foundation (1999), Research Project(s) About Enterprise-wide Risk Management, Sub-committee on Risk Management, IIA, Altamonte Springs, FL.

Irwin, D. (2007), *Why Do We Need Enterprise Risk Management?*, WIPFLi LLP, Milwaukee, WI.

King, J. (2001), *Operational Risk, Measurement and Modeling*, John Wiley & Sons, Chichester.

KPMG (1999), ''Control and risk self-assessment'', Presentation, Chicago, IL.

McNamee, D. and Selim, G. (1998), *Risk Management: Changing the Internal Auditor's Paradigm*, IIA Research Foundation, Altamonte Springs, FL.

Rasmussen, M. and McClean, C. (2007), *Demystifying Enterprise Risk Management*, Forester Research, Inc, New York, NY.

Robitaille, D. (2004), ''World-class audit and control practices'', *Internal Auditor*, February, pp. 75-81.

Securities and Exchange Commission (2002), SEC Proposes Additional Disclosures, Prohibitions to Implement the Sarbanes-Oxley Act, News Release 2002-150.

Further reading

AICPA (1995), *Statement of Auditing Procedures No. 78: Consideration of Internal Control in a Financial Statement Audit*, AICPA, New York, NY.

Corresponding author

Priscilla Burnaby can be contacted at: pburnaby@bentley.edu