SOCIETY OF ACTUARIES

Article from:

Risk Management

July 2005 – Issue 5

Developing Effective Risk Management Strategies to Protect Your Organization

by Fay Booker

Introduction

Enron, WorldCom, and Barings Bank are household names and, unfortunately, examples of what can go wrong in big business. With these high-profile business failures, people have asked why the boards of these companies did not do a better job of managing the risks. But was the board even aware of the nature and extent of the risks? Had the board identified the risks requiring active management and oversight?

Let's state up front that every business has risk. It is unreasonable to expect a company to organize itself and enact all necessary activities to eliminate risk. This would be cost prohibitive. However, by identifying the risks of the business and assessing the likelihood and impact of the risk, the company can make cost-effective decisions as to the appropriate risk response.

Managing risk has become a critical element within most companies. How that risk is managed, though, can be structured differently within companies even for those within the same sector.

This paper will look at the following topics:

- Successfully identifying, assessing and managing risks for all stakeholders.
- Identifying the appropriate strategy for your particular needs.
- Ensuring the governance body understands risk.
- Developing a risk management framework.
- Incorporating risk management into your business planning.

Successfully Identifying, Assessing and Managing Risks for Stakeholders

So what is risk? In the business world, the word risk has come to mean *an impediment to the achievement of an organization's objectives.* Risk management has become the mechanism to manage risks so that the negative consequences are kept within acceptable tolerances.

Some executives state that their organization employs an enterprise risk management (ERM) framework. What is ERM?

ERM involves a strategic analysis of risk across an organization. The view is corporate rather than silos—it cuts across business units and departments and considers end-to-end processes. ERM enables an organization to identify and evaluate its risk profile. Thereafter, the organization can determine appropriate responses to the risk profile, given the business environment and the organization's objectives and priorities.

Developing Effective Risk Management Strategies to Protect Your Organization

There are unique risks for each organization, given the nature of operations, although generally organizations within the same sector will have common risk elements. The appropriate risk response will be different from organization to organization, depending on how management views the risk in terms of magnitude. Risks are represented in the external environment in which the organization chooses to operate, as well as those in the internal environment. Risk factors in the external environment and generally outside of the organization's direct control include politics, the economy, regulations, natural disasters and competition. Examples of those within an organization's control include reputation, safety of employees, safeguarding of assets, ethics and culture.

As Figure 1 on page 28 shows, a risk management framework involves a continuous cycle of identify, assess, measure, decide response, assign responsibility, monitor, report and inform.

Step 1: Identify

The first step to implementing ERM requires explicitly identifying the risks that are inherent to the business and operations of the organization. There are different techniques that can be utilized to identify the inherent risk and

continued on page 28 ◗

Fay Booker, CA, CIA, is principal of Booker & Associates in Hamilton, Ontario. She can be reached at *fbooker@bookerandassociates.com.*

Developing Effective Risk Management Strategies to Protect Your Organization

◗ continued from page 27

therefore, the risk profile. Techniques such as self-assessment processes, completing surveys and facilitated risk workshops are generally used.

Facilitated risk workshops are a commonly used tool. The advantage of this mechanism is the ability to have workshops for different levels of responsibility, i.e., the governance level would have a different view of magnitude of risk than a front line staff member. Risk workshops also permit the inclusion of the greatest number of staff from across the organization, thereby increasing their awareness of risk and their participation in finding solutions and identifying approaches to managing the risks. Decentralized risk ownership will require risk evaluation at individual activity levels, with roll up to line of business or business unit, and then an overall evaluation for the organization.

Figure 1: ERM Circle

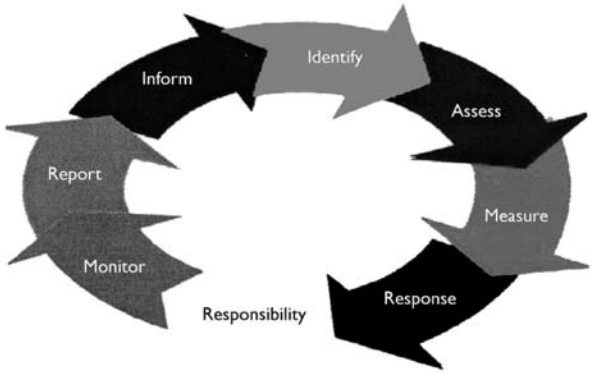


Table 1: Retail Company

Level/Role	Objective	Risks(s)
Board of Directors	Enhance shareholder value	Inappropriate strategy Excess infrastructure
CEO	Maximize net income	Underestimating competition Not attuned to consumer buying
Merchandising Manager	Maximize revenues	Goods don't arrive in time for season Goods don't reflect latest trend
Store Manager	Provide pleasant shopping experience for consumer	Insufficiently trained staff Store not appealing in appearance
Store Clerk	Minimize cash under	Illegal tender passed by consumer

Consider the nature of objectives and risks that those at different levels and in different roles within a company would focus on. Table 1 provides examples of objectives and risks, by level, in a company that operates a national chain of retail stores:

Step 2: Assess

The next step is to assess the risk on two dimensions: the likelihood of occurrence and the impact of occurrence. Tools are available to assist participants at this stage to indicate their view of the risk. A common tool used is voting technology whereby each participant is allowed to "vote" his or her assessment on an anonymous basis. The technology then compiles the results of all participants' votes on a defined scale and presents the results to the participating group. This allows the organization to identify if there is clear consensus on the assessment of risk or widespread views, thereby requiring further discussion and actions, possibly even training for the individuals.

The combination of the likelihood of the risk occurring, and the impact if it occurs, results in the degree of severity of the risk. Figure 2 on page 29 presents a graph demonstrating the collection of risks and the scale of risks with an organization.

Step 3: Measure

The organization needs to determine how the exposure will be measured. The measurement could be stated in different terms such as risk of financial loss through write-off of dollars or pay out of penalties or fines, risk of damage to business reputation or risk of loss due to inefficiency in processes.

At the end of step 3, risks will have been identified, measured and assessed as to the degree of severity. The resulting information from these steps is known as the risk profile.

A risk analysis process can capture information from the first three steps using a facilitated risk

workshop. Figure 3 below demonstrates the Risk Assessment Process.

Step 4: Decide Response
With the risk profile in hand, the next step is to determine what the appropriate response is to prudently manage the risk. The four risk responses include: avoid, accept, transfer, mitigate.

For each risk identified, the risk response can be articulated. It is expected that where the severity of the risk is high, there will be a strong risk response.

Every organization will have its own risk threshold. For example, where the risk response is to accept the risk, this becomes part of the organization's risk threshold.

Similarly if it is decided to accept risk to a certain dollar value, e.g., deductibility amount, this will be part of the risk threshold.

Step 5: Assign Responsibility
Each risk needs to be assigned to a position/person within the organization. The person responsible needs to ensure that the risk response is translated into actual day-to-day actions that will prevent and/or detect the risk. It will be this person's responsibility to manage the robustness of an insurance program, an outsourced arrangement, a policy statement, exception reporting, assignment of authorities, etc.

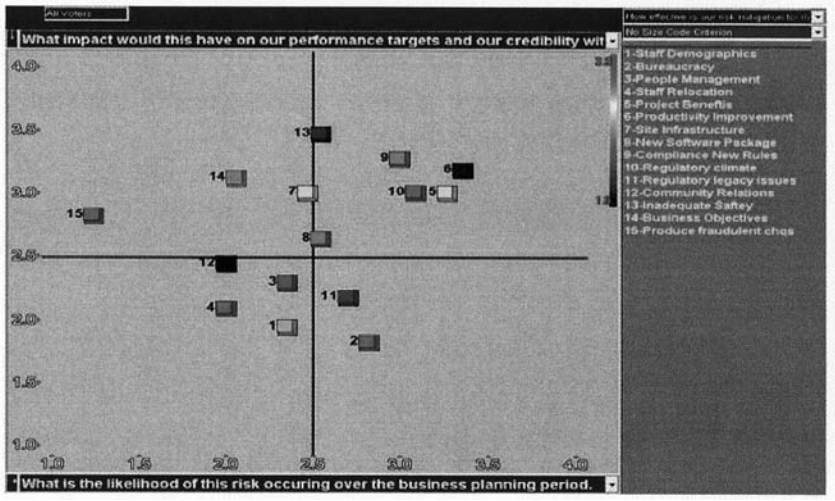
Step 6: Monitor
After implementation of the risk responses and management techniques, the managers need to monitor the actual activities to ensure that the identified risk stays within an acceptable threshold. Additionally, other units within an organization may take on a monitoring role. Some organizations have adopted centralized risk management groups, who have a responsibility to determine risk parameters and monitor actual results, to ensure that these parameters are honored. Internal audit also becomes part of the monitoring process, assuming the function is utilizing a risk-based internal audit approach.

Step 7: Report
The governance body and executive management will require information to be reported that allows them at their level of concern to be aware of the integrity of managing risks across the organization. Managers should determine the form of reporting necessary to best inform the oversight body.

Step 8: Inform
Information from the reports can be used to inform the annual update of the risk analysis

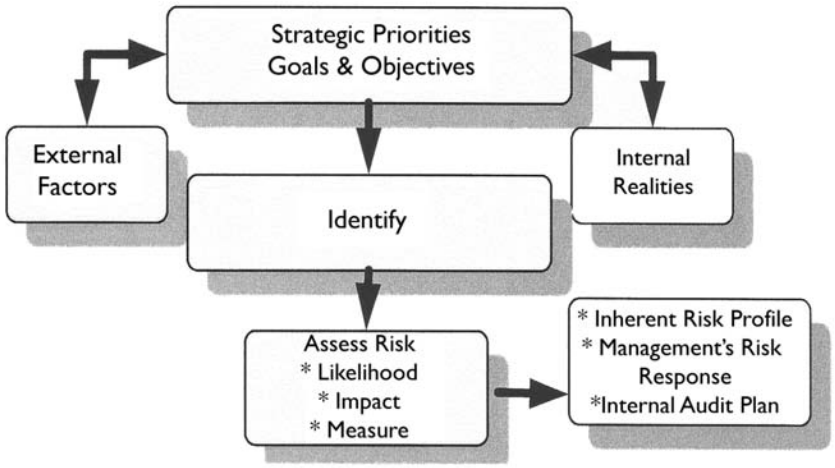
continued on page 30 ◗

Figure 2: Risk Graph[1]



[1] The graph is produced using The Revolver*Ballot® Risk and Control Self Assessment Software. Information on this tool can be found at *www.resolver.ca*

Figure 3: Risk Assessment Process



Developing Effective Risk Management Strategies to Protect Your Organization

◗ continued from page 29

Table 2: Responses

Avoid	This response is to not accept the risk, e.g. exit the business.
Accept	This response is to accept the level of risk and take no action to minimize it further.
Transfer	This response is to transfer the risk to someone else, e.g. puchase insurance.
Mitigate	This response is to take action to manage the risk generally through a system of internal controls.

process, as well as the updating of risk responses and policies. Risk management is a continuous process and also a continuous improvement process.

Identifying the Appropriate Strategy for Your Particular Needs

Some companies have adopted a centralized model for risk management, while others are using a decentralized model. The approach depends on an organization's particular operations, the significant risks, the culture of the organization, the management style and the control environment, i.e. the degree of centralization or the delegation of authority and the infrastructure of the business.

In a centralized model it is the risk management department that develops policies for the board to consider. Included in the policies will be decisions on the amount of risk to be taken. Thereafter, the authority for making the risk decisions is with the risk management department as is monitoring and reporting on the risk. The line staff provide the source information to the risk management decision makers.

Other organizations have decentralized operations requiring the involvement of front line staff in managing the inherent risks of the company, of the business unit or of the process. This model requires staff education, clear understanding of the need to adhere to control practices, accountability in job descriptions and mechanisms for senior management to identify and aggregate the risk exposure.

Ensuring the Governance Body Understands Risk

Risk management is one element of robust corporate governance but, like anything else, in order to be effective, there must be a solid understanding by those with the oversight responsibility.

Following is the standard that the Canada Deposit Insurance Corporation, the regulator of the financial institutions, has set for the governance level.

It is a sound business and financial practice for the board of directors to:

1) Understand the significant risks to which the institution is exposed.
2) Establish appropriate and prudent risk management policies for those risks.
3) Review those policies at least once a year to ensure that they remain appropriate and prudent.
4) Obtain, on a regular basis, reasonable assurance that the institution has an ongoing, appropriate and effective risk management process and that the institution's risk management policies for significant risks are adhered to.

The Canadian securities administrators have identified similar responsibilities for boards of directors.

The first element, which requires understanding of the significant risks, can be accomplished through presentations from executive management on the analysis of the risk profile of the company. Additionally, the governance level can participate, with executive management, in a facilitated risk workshop to articulate and discuss the risks which are inherent to the business, products and services.

Once informed on the significant risks, the board can then direct management to develop policies for the board's consideration. Being informed will enable the board members to sufficiently consider and conduct due diligence on

draft policies. The annual review process should consider changes in the external business market, changes within the company and changes to the company's strategic objectives.

The most significant element of the standard is to "obtain reasonable assurance that the institution has an ongoing appropriate and effective risk management process and that the institutions' risk management policies for significant risks are being adhered to." This is a significant obligation indeed. So how do boards gain reasonable assurance?

Different tools should be made available to the governance level. The CEO can be requested to provide information that demonstrates the ongoing active management of the risks. Increasingly, audit committees are being delegated responsibility for overseeing risk management practices of the organization. This responsibility requires support from within the organization, and the vehicle that is commonly selected is the internal audit function. Given the independence of the internal audit function, it is seen as a means to provide the governing level with an independent assessment of the appropriateness and effectiveness of the risk management practices.

Following is an extract from the terms of reference of an audit committee outlining their responsibilities for risk management.

Risk Framework

The audit committee will ensure that there is proper understanding by the board of the risks of the company and the specific risks of products and processes. The audit committee will:

- Understand the risks associated with the business that the company provides and ensure that appropriate means are in place to manage these risks.
- Review and recommend prudent risk management policies to the board.
- Receive from management ongoing reports on operation of risk management practices and risk thresholds.
- Receive from the internal audit function periodic reports on the effectiveness of risk management practices.

As a key supporting resource to the governance level, and in particular the audit committee, internal audit functions are being asked to take on greater responsibility in the area of risk assessment and risk management activities. However, this responsibility cannot be imposed on the internal audit function unless it has the competency and capability to undertake this significant assignment. It is a simple task to update the internal audit function's mandate to include responsibility for assessing risk management, but it is a more considered task to ensure that the function is capable of undertaking the responsibility.

Developing a Risk Management Framework

So how does a company develop a risk management framework appropriate to its business and nature of operations? Before establishing a framework and undertaking process, the following elements must be in place to permit effective risk management:

1) *Support at senior levels:* The need for risk management must start and be supported at the highest level within the company. This includes the governance level and the CEO. The support must be genuine.
2) *Proactive not static:* Risk management efforts must be proactive. This involves the active identification, measurement and management of the risks, scanning of changes in the risk profile and reports on managing the risk profile.
3) *Clarity of understanding:* There needs to be a clear definition of the risks, and these must be understood across the organization.
4) *Accountability:* Responsibility for responding to and managing the risks must be clearly understood and individuals held accountable for fulfilling the roles. Managing risk must be seen as part of every process and position.
5) *Resources:* Appropriate resources including people and tools need to be deployed and available to help managers, executive and the governance level conduct their obligations within the risk management framework.
6) Culture: The organization's culture must provide for the active management of risk.

continued on page 32 ◗

Developing Effective Risk Management Strategies to Protect Your Organization

◗ continued from page 31

Once a company has decided that it will support each of these elements, a champion within the organization can be selected to start the process to identify, measure, assess, etc., and thereafter ensure the continuance of the process.

Incorporating Risk Management into Your Business Planning

Risk identification should be an explicit step in a company's strategic planning cycle. This would require consideration of those risks that might arise in the longer-term planning horizon. Identification of the emerging risks during strategic planning will be more important than acknowledging the current risks inherent to the business. The anticipated impact of emerging risks may render the business or products obsolete and, therefore, signal very aggressive responses such as innovation or divestment.

Consider the following[2]:

A DIRECTOR'S STORY: As I head into retirement and look back on my career as an independent director, I realize that my efforts were mostly futile. I think especially of my time as a director of a financial institution that failed. Management gave us reams of information about past performance and we dutifully discussed it. We were looking at the wrong information and asking the wrong questions. We should have focused on the future and questioned the strategy and the competence of management to execute it. That's what caused the institution to fail and the board didn't wake up until it was too late.

At each level of planning in a company's annual business planning process, there should also be an examination and analysis of risks, current and emerging. This consideration for risk should be conducted at unit level and department level, as well as enterprise level. The risks should be examined and the responses determined. The response may translate into specific marketing or selling actions, or even financing decisions. The business plan can capture these considerations and provide for an informed company, governance and management level to proceed in an organized prudent manner.

Summary

Risk management is a discipline that can assist in the success of an organization. Like anything that pays dividends, it takes knowledge, commitment and support to provide the greatest benefits to an organization.

The greatest reward should be a shift from reacting to crisis to being aware of and managing risk. Being in control, having structure and being organized allows for a business environment that is empowering and permits taking advantage of opportunities. It also allows for a knowledgeable and learned employee group and governance body.

Hopefully risk management is a factor in ensuring that your organization is well known for its success. ✦

[2] CICA, Guidance for Directors – Dealing with Risk in the Boardroom, April 2000.