Discussion Paper

BOOKER & ASSOCIATES

Developing Effective Risk Management Strategies to Protect Your Business

Prepared by:

Fay Booker, FCPA, C. Dir., CIA, CRMA, Acc. Dir.

Principal, Booker & Associates

www.BookerandAssociates.com

fbooker@bookerandassociates.com

Introduction

Names like Enron, Worldcom, Barings Bank and Menu Foods are household names but unfortunately as examples of what can go wrong. With these recent high profile business failures, people have asked why the Boards of these companies did not do a better job of managing the risks. But were they even aware of the nature and extent of the risks? Had they identified the risks?

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. 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 your 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?

Enterprise risk management involves a strategic analysis of risk across an organization. The view is a corporate one rather than a silo one – 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.

There are unique risks for each organization given the nature of operations although generally organizations within the same sector will have common risk elements. How management of the business views the risk in terms of magnitude and appropriate risk response will be different from organization to organization.

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, geographic (natural disasters), and competition. Examples of those within an organization's control include reputation, safety of employees, safeguarding of assets, ethics and culture.

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

Exhibit I: ERM Circle

Step 1: Identify

The first step to implementing ERM requires identifying the risks that are inherent to the business and operations of an organization. There are different techniques that can be utilized to identify the inherent risk and therefore the risk profile of an organization. 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, then an overall evaluation for the organization.

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

Exhibit II: Retail Company

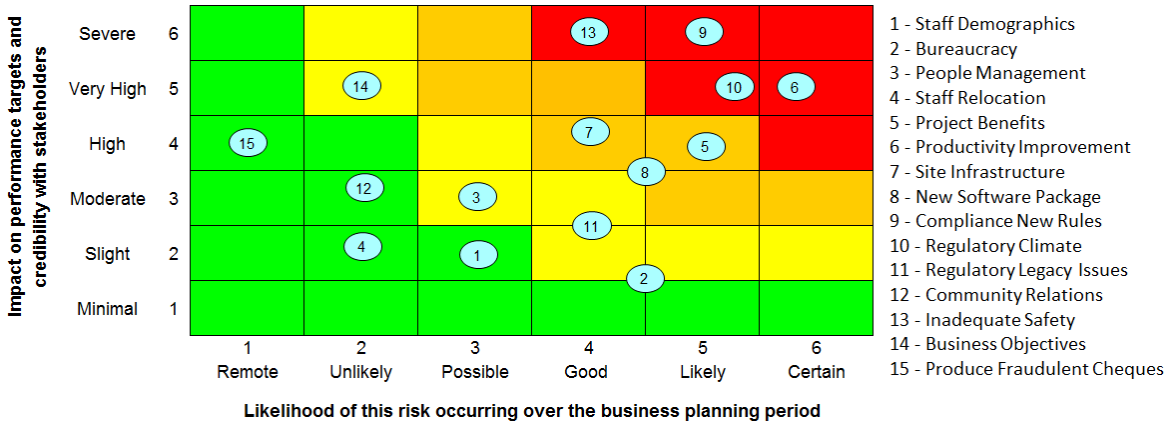
Level/role	Objective	Risk(s)
Board of Directors	Enhance shareholder value	Inappropriate strategy Excess infrastructure
CEO	Maximize net income	Underestimating competition Not attuned to consumer buying
Merchandising manager	Maximize revenues	Goods don't arrive in time for season Goods don't reflect latest 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

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 issues or wide spread assessments, thereby requiring further discussion and actions, possibly even training for the individuals.

The combination of the likelihood of occurrence and the impact of occurrence results in the degree of severity of the risk. Exhibit III presents a graph demonstrating the collection of risks and the scale of risks with an organization.

Exhibit III: Risk Graph



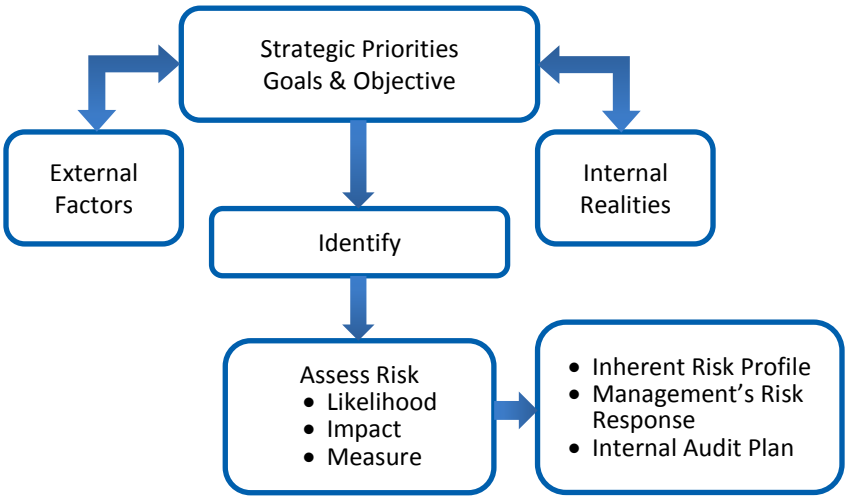
Step 3: Measure

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 payment 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 facilitated risk workshops. Exhibit IV illustrates the elements of the risk assessment process.

Exhibit IV: Risk Assessment Process



Step 4: Assign 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.

Exhibit V

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, e.g. establish reserves.
Transfer	–	this response is to transfer the risk to someone else, e.g. purchase insurance.
Mitigate	–	this response is to take action to manage the risk generally through a system of internal controls.

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: Responsibility

Each risk is assigned to a position/person within the organization. The responsible person 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 honoured. Internal Audit 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. Additionally Internal Audit needs to structure their reporting to follow a risk focus.

Step 8: Inform

Information from the reports can be used to inform the annual update of the risk analysis 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).

The major financial institutions in Canada typically have a centralized model. They have central Risk Management departments with significant responsibility within the institution. It is the Risk Management department that authors policies for the Board to consider. Included in the policies will be decisions on the amount of credit risk to be taken, the extent of interest rate risk, etc. Thereafter the authority for making the credit decision or the interest rate decision is with the Risk

Management department. The line staff process the information that is provided 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, the business unit, or the process. This model will require 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 exposure of risk.

Ensuring your 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:*
>
> *a. understand the significant risks to which the institution is exposed,*
> *b. establish appropriate and prudent risk management policies for those risks,*
> *c. review those policies at least once a year to ensure that they remain appropriate and prudent;*
> *d. 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 being 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?

There are different tools that 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 processes.

Following is an extract of an element from the terms of reference of an Audit Committee outlining their responsibilities for Risk Management.

Risk Framework

The Audit Committee will ensure there is proper understanding by the Board of the risks of the company and the businesses operated by the company. The Audit Committee will:

- *understand the risks associated with the type of business that the company provides and ensures 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.*

Internal Audit functions are being asked to take on greater responsibility in the area of risk assessment and views on 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.

Following is an example of a role description for an Internal Audit function.

Role

It is the role of Internal Audit to be an integral part of the risk management framework of the company. The risk management framework recognizes that risk is inherent to the business and operations of the company, and it is management's responsibility to design internal controls and operate such controls that will mitigate that risk. Internal Audit has a role within the

framework to be part of the risk management strategy and to work with management and the Audit Committee in supporting their roles in the framework.

The role of the Internal Audit function is:

a. *To provide to the Audit Committee an evaluation of the adequacy of the internal control structure for the company in relation to the risk profile.*
b. *To support the Audit Committee in discharge of its governance responsibilities.*
c. *To provide to management an evaluation of the adequacy of their control processes and to provide input to the design, development and implementation of those systems without compromising the independence of the function.*
d. *To provide management with other specialist services based on its expertise in the control systems and processes of the company.*

It is incumbent on the Internal Audit function to utilize an appropriate internal audit methodology that will provide the focus and consideration of risk as envisaged and required in supporting the Audit Committee.

I have seen Internal Audit functions being expected to rise to the level of being an effective element of the risk management framework only never being provided with the resources to execute on this responsibility. Audit methodology for Internal Audit has had to evolve as it has for the external audit profession. The old compliance method of auditing has been replaced with a more sophisticated risk-based and risk-driven planning and auditing perspective. To best serve the sponsoring organization, the Internal Audit function must first understand the business. This understanding must include understanding the inherent risks to the business, the products, the competition, how the product is delivered and the operations.

Reports from the Internal Audit function need to be appropriate to the role and responsibility of the group to whom they are presenting. Reporting to Audit Committees and Boards of Directors requires the internal audit function to provide an enterprise-wide view. At the senior levels it is important for the Internal Audit Director to provide an opinion on the state of the internal controls across the organization. The Board needs to be apprised if there is evidence that the control structure is weakening or if certain risks are not being adequately mitigated.

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: Concern 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 reporting of the success of 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 support the active managing of risk in terms of attitude.

Once a company has decided that they 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.

There are specific responsibilities in an ERM framework that are assignable to the Board and to management.

Board Responsibilities in ERM	Management Responsibilities in ERM
Understand the company's risk profile	Build the risk profile
Develop governing policies in areas of specific risk	Determine the appropriate risk responses and allocation of resources
Ensure strategic planning process includes an analysis of emerging risks	Enact practices to mange the risks
Ensure periodic update of risk profile, assessment of risks and risk responses	Hold people accountable to their assigned responsibilities
Set and reinforce the tone for corporate ethics and control culture	Inform the Board on the risk management practices and levels of risk
Focus the Board's time and attention in the areas of highest risk	Update the Board as the risk profile changes

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.

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, 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 providing for 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, 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 known for its success.

Booker & Associates promotes excellence in Corporate Governance, Risk Management and Operational Effectiveness. Since 2004, we have worked with organizations across Canada to provide solutions that lead to substantial results.

Booker & Associates provides services to support Boards in exercising good governance including governance education programs, governance coaching, Board and Director evaluation processes, governance policy writing, and strategic planning facilitation. We provide training on Enterprise Risk Management, facilitate risk workshops, and assist organizations in building risk frameworks, accountabilities, and measurements.

Visit our website at www.BookerandAssociates.com