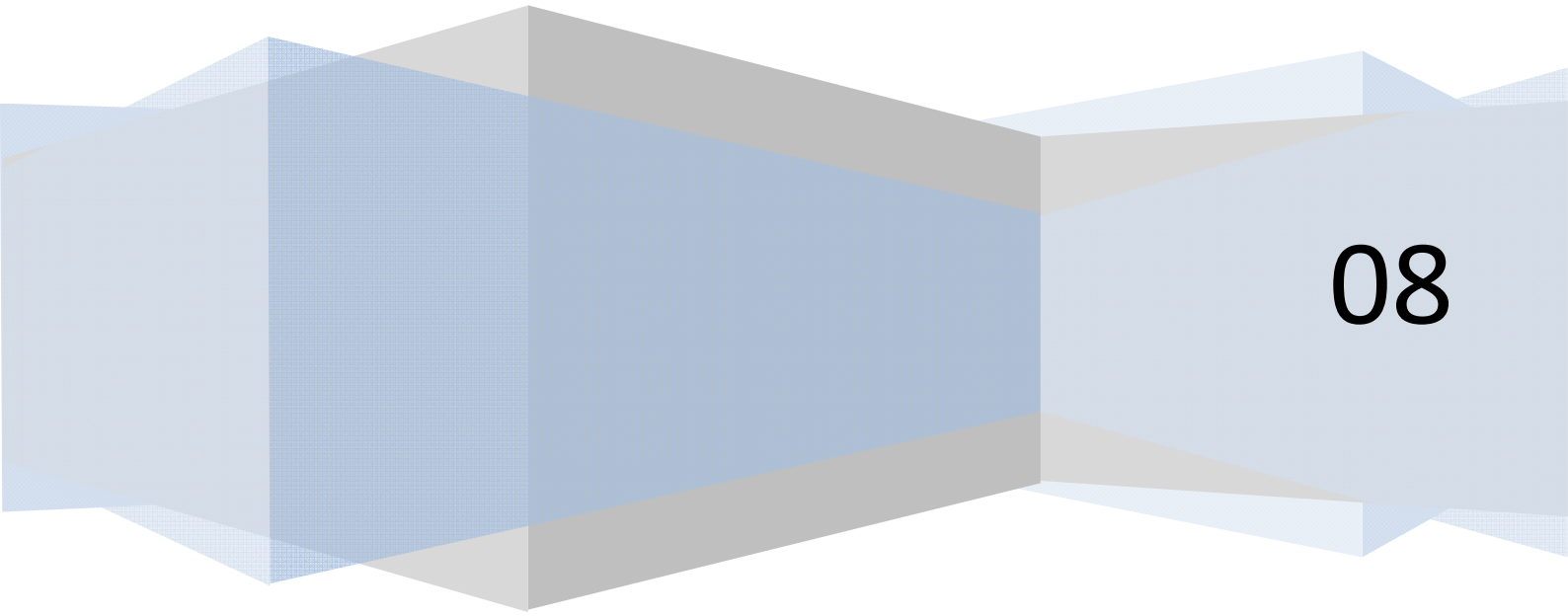
Enterprise Risk Management

BADM 458 – IT Governance

Portia Woodhouse



08

Table of Contents

Introduction

Every business is challenged with uncertainties that would present threats to its success. This, known to many as risk, "is defined as the probability of an event and its consequences" (Cranfield School of Management). The main categories of risk to consider in a business environment are strategic, compliance, financial, and operational. All of the aforementioned categories are different branches of a business that drives a company's success. If one area faces risk, it could put the whole company at danger. Companies are challenged with questions on how to mitigate risk with every decision that they make. Most businesses strive to keep their stakeholders happy by growing and changing in order to compete with other firms. Every time the business makes a decision to increase its offerings, take on new employees, revise marketing tactics, expand into new areas of business beyond its core business, a degree of risk does arise. Various tools, methods, and assessments are performed to control such threats. This is known as risk management.

Organizations have for many years practiced various methods of risk management. It has evolved from traditional risk management, to now, what most companies are practicing, enterprise risk management. There is a fine distinction between the two approaches. This research report will focus on the most recent approach used throughout many companies today, enterprise risk management. As this approach is explained, the following topics will be addressed: evolution of risk management, enterprise risk management framework, driving forces behind enterprise risk management, and enterprise risk management best practices.

Evolution of Risk Management

In today's business environment, past risk management practices are no longer sufficient to moderate today's threats. There are new levels of threat that exist that weren't in existence years ago. Unrelated items, including heightened competition, natural disasters, fuel dependency, terrorism, and government regulatory policies such as Sarbanes-Oxley, are a few which conspire to create a new altitude of risk for businesses. In addition, the rapid change in the technological environment creates a new risk factor as well. Consequently, the ability for companies to discreetly control a risk matter has, in reality, vanished. Worst case scenario to this issue could be the company's brand and reputation plummeting (Layton and Wagner).

Traditional Risk Management

The traditional risk management approach has been characterized as a highly disaggregated method of managing a firm's risk. Under this approach, various categories of risk are managed in separate units within the firm. Financial firms, for example, often manage market, credit, liquidity, and operational risk separately in individual risk silos. Traditionally, non-financial firms have followed a similar approach to hazard, financial, operational, and strategic risks.

This form of risk management has a lot of weaknesses, which have caused a lot of companies to look for a better approach. According to Steve Wagner, a managing partner at Deloitte & Touche, "the inability to deal with risks of all types has resulted in a dramatic increase in CEO and CFO turnover. More worrisome, the failure to successfully manage risk can result in personal liability, as evidenced by recent out-of-pocket settlements paid by board directors."

Among all of the issues traditional risk management encompasses that inhibit effective and efficient risk management, the "silo factor" is amongst the most significant. Normally, risk is allocated to risk managers within departments. As mentioned above, a great illustration of that

would be the finance department examines credit risk, public relations monitors reputation risk, and IT observes data security risk. Granted, this level of specialization is very important, grouping risk managers in these silos results in a limited view of risk. In addition, it also hinders top management from understanding risk as it affects the whole company. A threat that affects one part of the business can cause an attack on another division. In example, an IT security breach can quickly turn into a reputational risk in the form of negative publicity. This shows that risk can combine and cause an even greater threat to the company. In most cases, this risk is difficult to repair (Layton and Wagner).

Another drawback of traditional risk management could be a company's misunderstanding of what risk management entails. Most organizations have only used half of the benefits risk management has to offer. To explain, they have only contemplated the negative affects of risk (those parts that could potentially jeopardize their current assets, such as IT security breaches, financial deception, and tangible resources). From the experience of Steve Wagner, "far fewer organizations apply the principles of good risk management to "upside" opportunities, such as product development, entering new markets, and merger and acquisition activities." Failure to effectively manage the risk in these activities could possibly cause severe and unanticipated damages. A few public companies have reported losses elevated to the billions because they didn't fully understand the benefits associated with risk (Layton and Wagner).

Enterprise Risk Management

Recognizing and prioritizing risk, either by proactive or reactive risk plans, has been a standard management activity. Since the beginning of the twenty-first century, however, there has been a fundamental shift in the way businesses approach risk. Organizations now treat " the vast variety of risk in a holistic manner, and [elevate] risk management to a senior management

responsibility" (Casualty Actuarial Society). This approach is quite different from the traditional approach. To outline those differences, the following section will discuss the driving forces behind Enterprise Risk Management that differentiates itself from the traditional approach.

ERM Framework

The primary goal of enterprise risk management is to ensure every entity provides value for its stakeholders. Every function (entity) of a company is challenged with uncertainty. The test for management is to decide how much uncertainty is okay. Value is exploited when management sets a strategy and objectives that create a balance between growth, return goals, and related risks. COSO states, enterprise risk management seeks to align risk appetite and strategy; enhance risk response and decisions; reduce operational surprises and losses; identify and manage multiple and cross-enterprise risks; seize opportunities; improve deployment of capital. Such capabilities assist management in achieving an entity's highest performance and profitability goals; also inhibits the loss of resources.

Objectives

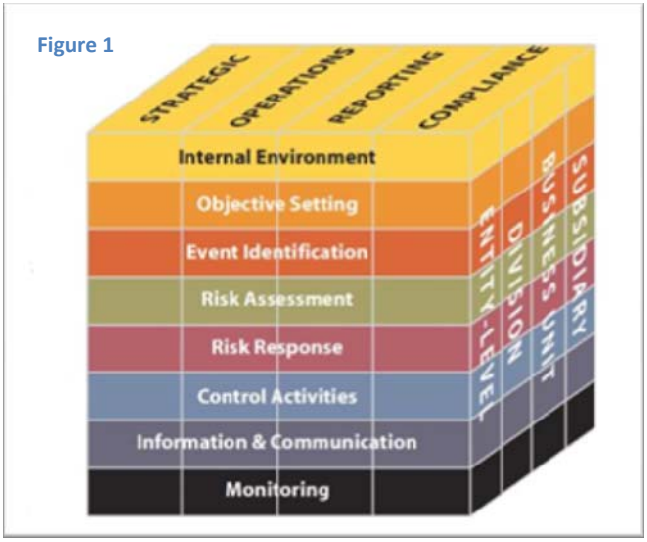
Again, there are four objectives enterprise risk management address. The first, strategic objectives are high-level goals that are aligned with and support an entity's mission. Second, operational, involves achieving effective and efficient use of resources. Third, reporting objectives focus on the dependability of reporting. The last objective, compliance, goal is to adhere to applicable regulations, policies, and laws.

Components

Enterprise risk management makes improvements to every area of the business; all levels of the organization are affected. A way to conceptual ERM is by thinking of it as a strategic decision support framework (see figure below). There are eight interrelated components. The first, internal environment, involves the tone of an organization, and sets the rules in which risk is evaluated and addressed by the entity's people. Second, objective setting, states objectives

must be present in order for management to identify potential events affecting their success. ERM ensures there's a process in place to set objectives. The third component, event identification, takes a look at internal and external events that could possibly affect the success of an entity's objectives. Objectives should be identifiable and distinguished between opportunities and threats. The fourth, risk assessment, is where risks are analyzed to determine how they should be managed. Risks are evaluated on a residual and inherent basis. Fifth, risk response, management determines how to respond to risk. They decide whether to avoid, accept, reduce, or share risk. The sixth component, control activities, includes policies and procedures that are created and implemented to guarantee risk responses are executed successfully. Seventh, information and communication, is where useful information is detected, captured, and shared in a form and timeframe that allow people to perform their responsibilities. Lastly, monitoring is where enterprise risk management in its entirety is examined and modified, if necessary. "Enterprise risk management is not a serial process, where one component affects only the next. It is a multi-directional, iterative process in which almost any component can and does influence another" (Committee of Sponsoring Organizations of the Treadway Commission).

Figure 1



Relationship of Objectives & Components

There is a direct relationship between objectives and enterprise risk management components. The objectives are what an entity works hard to accomplish. The enterprise risk management components are necessary to attain them. The three-dimensional cube (figure 1) illustrates this relationship. The objective categories are illustrated by the vertical columns; the ERM

components, by the horizontal rows; and an entity's unit is represented to the third dimension. Figure 1, shows how a company's risks can be examined in it's entirety, by entity unit, or objective category.

Effectiveness

In determining the effectiveness of an organization's enterprise risk management model, the eight components of ERM must be examined to insure they are present and working correctly. With that said, the eight components are also used as the criteria for a company's ERM model. When examining the effectiveness, an organization's model is tested for material weaknesses. In addition, risks must be examined to ensure they are within the company's risk appetite. When it is determined that ERM is effective in each of the four categories, the board of directors are assured that they have recognized the length to which the entity's strategic and operation objectives are being met. It also indicates that the entity's reporting is reliable and relevant laws and regulations are being fulfilled. It is good to mention that the eight components will not function the same in every entity (Committee of Sponsoring Organizations of the Treadway Commission).

Limitations

Enterprise risk management offers many benefits, however, limitations do exist. Limitations derive from the realities that human decision-making can lead to bad judgment; relative cost and benefits could go overlooked when responding to risk and creating controls; human errors can cause breakdowns to occur; ERM decisions can be overridden by management. Such limitations inhibit the assurance to board member and directors that they have achieved the entity's objectives (Committee of Sponsoring Organizations of the Treadway Commission).

Internal Control

Internal control is an important element of enterprise risk management. ERM framework covers internal control and other useful concepts and tools. The internal control portion of the ERM framework is derived from the Internal Control - Integrated Framework. This framework has been around for a long time and is the beginning point for existing rules, policies, documents, regulations that are in place for the definition of and framework for internal control. Only portions of the internal control framework are integrated in the ERM framework (Committee of Sponsoring Organizations of the Treadway Commission).

Roles & Responsibilities

Everyone throughout an organization has some responsibility for enterprise risk management within their respective entity. The chief executive officer is ultimately responsible and should take ownership of the company's ERM model. The CEO's close subordinates (management team) has the responsibility of supporting their entity's risk management philosophy, encourage adherence with its risk appetite, and manage risks within their role as manager over their team. In addition, a risk officer, internal auditor, financial officer, and others normally have important supporting roles. Other entity personnel are responsible for adhering to ERM protocols. The board of directors administers the ERM model at the organization and is aware of and agrees with the entity's risk appetite. External parties (customers, vendors, business partners, regulators, external auditors, etc) are not responsible for the usefulness of the organization's enterprise risk management mode. They do, however, supply information that is helpful for the delivery of an ERM model.

Driving Forces behind ERM

More Complicated Risks

Organizations are now recognizing more than ever before the variety, increasing number, and interaction of risks they are faced with. Financial risk's importance has grown over the past few years. Hazard risks, such as the possibility of a production facility setting afire has been actively managed for quite some time. New threats have surfaced with the rapid changes in the business environment. The awareness of strategic and operational risks has risen due to a number of high-profile cases that were destroyed. One company in particular, Enron, suffered huge damages due to the lack of control mechanisms. The complexity of risk expands across many spectrums: advances of technology, globalization, and uncertainty of terrorist activity. The categories of risk will continue to increase. Companies realize the how imperative it is to manage all risks, and their interactions with one another (Casualty Actuarial Society). Unlike ERM, traditional risk management's structure does not allow for such an integrated approach to control risk. Funneling risk down more than one pipe doesn't communicate the interactions and holistic risk associated with all of the functions of a business.

External Pressures

As a result of the widely publicized cataclysmic failures of corporate risk management discussed above (Enron), government regulators, rating agencies, institutional investors, stock exchanges, and corporate governance supervising firms have demanded that company's senior leaders taker more responsibility for controlling risk on an enterprise-wide level (Casualty Actuarial Society). Enterprise-wide risk is something traditional risk didn't address. The pressure felt by companies after the downfall of a few well-known companies was definitely key in businesses migration to ERM.

Portfolio Point of View

Another driving force is the movement toward a holistic analysis of risk. Modern theories of finance (e.g. Modern Portfolio Theory) offer a framework for assessing the collective risk of a group or individual financial risk. With ERM, these concepts have been generalized to include all types of financial risk. These concepts are having a substantial bearing on the practice of ERM. Organizations are learning to manage risk without the total organization in mind is inefficient management practice. "A holistic approach helps give organizations a true perspective on the magnitude and importance of different risks" (Casualty Actuarial Society).

Qualification

This driving force is closely tied with the previous. Advancements in technology have made quantification much easier, even for less frequent, unpredictable risks that have been difficult to quantify in the past. After subsequent natural disasters, the practice of catastrophe modeling surfaced. It is now a standard procedure for insurance companies. According to the Casualty Actuarial Society, "the combination of meteorological, structural engineering, insurance and technological expertise leading to probabilistic models is a huge advancement over previous quantification attempts." Of late, such exposure-based quantification of visibility to losses had been used to predict man-made disasters like terrorist attacks. The financial services industry had also been aided with a regulatory and management standard that assists in measuring certain financial risk: value-at-risk. With this tool, data is gathered constantly, which allows risk profiles to be changed as portfolios and the state of the market changes. The confidence embodied in the process gives financial institutions and regulatory firms the chance to take actions to work within established borders (Casualty Actuarial Society).

Although advances have been made, less quantifiable risk will always exist. This includes risk that isn't well understood, unpredictable (frequency), size or location, and unforeseen risks (new

risks). Examples of new risks include strategic, man-made, and operational. The latter is a general class for a number of risks (Casualty Actuarial Society).

Boundaryless Benchmarking

This driving force relates to scope. Universal Enterprise Risk Management practices and tools are shared throughout a number of organizations and companies across the world. Information sharing has been supported by technology and the ease of transferring information across organizations. The development and employment variations of ERM will continue to exist throughout different industries and organizations. While it may be true that there will be a difference in risk, their importance to organizations, and the risk management practices, the general concepts and techniques will be recognized by organizations, globally (Casualty Actuarial Society).

Risk as Opportunity

The last driving force behind Enterprise Risk Management involves the organizations perception of risk. As mentioned earlier, traditional risk management viewed risk as conditions to minimize or avoid. However, organizations have come to realize the opportunities and value-creating possibilities of risk. Minimizing and avoiding risk are valid strategies for controlling certain risks. On the other hand, when the opportunity permits, certain organizations can swap, keep, or actively pursue other risks because they have assurance in the organization's capability to take advantage of those risks. Organizations have become more comfortable and capable of controlling risk associated with their business. Organizations now establish experts who can manage those risks with confidence and familiarity. The Casualty Actuarial Society asserts, "In some cases organizations seek out risks to increase diversification, realizing that the addition of some risks may have a minimal impact on overall risk, or in the case of hedges, may decrease

enterprise risks." Organizations realize it is difficult to completely avoid risk, so they find the best way to mitigate it.

Best Practices

Companies recognize the value enterprise risk management offers their organization. Risk is an issue every business is challenged with. CEOs, CFOs, and members of senior management are constantly challenged with various levels of regulatory policies, shareholder demands, and business complexities. The discipline that has been most helpful in tackling these problems is the discipline of enterprise risk management. According to Mark Layton, “a recent study in Fortune magazine of S&P 500 companies showed that overall risk levels more than doubled between 1985 and 2006.” Implementing enterprise risk management has helped companies significantly reduce their exposure to risk. In this section, some of the ERM’s best practices will be examined.

ERM Systems

During enterprise risk management’s inception, the software tools necessary to effectively implement ERM were the responsibility of the company. Third party applications were very inadequate. Thus, companies were forced to develop in-house software solutions. This, however, isn’t the case anymore. Steven Mininsky, CEO and founder of LogicManager Inc. (ERM software solutions provider), believes it is a bad decision to develop your own software packages. Steven claims homegrown applications are expensive to build and maintain nowadays.

JPMorgan Chase, a well-known financial institution, created an internal enterprise risk management system. Although the system was successful, the company incurs tremendous yearly expenses. They employ over 55 development and supporting staff to maintain the

system. In addition, the company is faced with multi-million dollar annual expenses. While the organization realizes the benefits of their internal ERM system, the expenses are not acceptable (Minsky).

As technological advances increase, enterprise risk management systems are constantly evolving. Consequently, solutions created internally, like JPMorgan's, become outdated very quickly. Furthermore, these systems cater more toward compliance and audit and sometimes overlook delivering value to the business (Minsky). ERM systems should meet the needs of and add value to every aspect of the business. Managers from every unit of the business should be involved in software selection to ensure this is accomplished.

Strategy & Planning Process

Risk management should be embedded within business processes. One in particular, the strategic and planning process, should encompass risk management. Organizations that practice integrating risk management with their strategy are able to enjoy a smooth process to goal attainment. If organizations examine the opportunities and threats of risk, they will be able to better assess their chances of successfully attaining their strategic objectives (Francis and Paladino).

Blue Cross Blue Shield Florida (BCBSF), a health insurance company, assesses strategic risk every year. This is executed by performing one-on-one discussions and independent assessments. The list of strategic risk gathered is then used as complementary information for strategic planning. The degree in which ERM is embedded within this process is different for each organization. Unlike BCBSF, other companies assess this risk weekly, monthly, or quarterly. As BCBSF embarks on their model, they also seek to dive risk management to

operational areas. This is accomplished by mapping strategic threats to operational planning through its plan and budget process (Francis and Paladino). This allows the company to integrate other aspects of the business into the risk management process of one function. Risk can then be assessed from a micro or macro level.

Risk Identification

In late 2007, a team of MBA students at Saint Peters College was given an assignment in which they had to identify critical risk factors Chrysler Corporation was challenged with. The team a collection of events accounted for Chrysler's risk. First, Cerberus, a capital management firm, acquired Chrysler after DaimlerChrysler couldn't recover from rough times. Cerberus then brought in Robert Mardelli as CEO. His management style was very controversial and brought on public attention when he was CEO of Home Depot (Hampton).

As the team took into account the aforementioned chain of events, they made several observations. The team classified the new CEO as critical leadership risk. They questioned whether his management skills would help or hinder the company. Other risks observed includes: general vs. specific risk and short vs. long-term risk. Risk identification, as performed by the MBA students, and creating a consensus on these risks is a good exercise to practice at any firm. It is actually the starting point of enterprise risk management at the governance level. According to John Hampton, a specialist in ERM and KPMG professor, ERM can begin at any place, but the three approaches that are emerging include governance, strategy, and performance. Beginning with governance, a company can identify the scope of their risk.

Conclusion

Enterprise risk management has become a very useful framework for many companies. The different tools, assessments, and business improvement models it offers continues to assist

companies with predictable and unpredictable threats. As the business environment continues to evolve, so will the ERM systems many companies use. It is important that companies stay abreast and knowledgeable.

Works Cited

Casualty Actuarial Society. "Overview of Enterprise Risk Management." May 2003. University of California Office of the President. 23 April 2008 <http://www.ucop.edu/riskmgt/erm/documents/overview.pdf>.

Committee of Sponsoring Organizations of the Treadway Commission. "Enterprise Risk Management - Integrated Framework." September 2004. Committee of Sponsoring Organizations of the Treadway Commission. 15 April 2008 <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf>.

Cranfield School of Management. "Managing Risk." 2008. Business Link. 25 April 2008 <http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1074404839>.

Francis, Sebastian and Bob Paladino. "Enterprise Risk Management: a Best Practice Approach." Journal of Corporate Accounting and Finance 19 (2008). Wiley InterScience. EBSCO. University of Illinois, Urbana. 29 Apr. 2008 <http://www3.interscience.wiley.com.proxy2.library.uiuc.edu/journal/11792288>.

Hampton, John. "Governanca a Start for ERM." 2008. Business Insurance. 27 April 2008 <http://www.businessinsurance.com/cgi-bin/page.pl?pageId=873>.

Layton, Mark and Steve Wagner. "Traditional Risk Management Inadequate To Deal with Today's Threats." March 2007. International Risk Management Institute, Inc. . 20 April 2008 <http://www.irmi.com/expert/Articles/2007/Deloitte03.aspx>.

Minsky, Steven. "The Dos and Don'ts of Enterprise Risk Management." 13 March 2006. ebizQ. 20 April 2008 <http://www.ebizq.net/topics/int_sbp/features/6791.html?page=3>.