The Fallacies and Future of Enterprise Risk Management

By Bruce B. Thomas

Not long ago, senior executives in large companies could feel confident that they had scaled the heights of enterprise and work in relative comfort. These days, unprecedented change impacts every aspect of the business environment. Whether it is pace of technological innovation, the preferences of fickle customers, or a legal and regulatory environment that has run amuck, creative destruction is the rule.

Today, senior executives might as well be sitting on top of Mount Everest. The rewards for making the right decisions are much greater than ever before, but the punishment for failure is just as steep. It seems that almost every week a large, venerated company that was the star of its industry has fallen on hard times and is struggling to survive. In recognition of the many perils they face, executives are searching for some theoretical or organizational framework to help manage their companies' risk. This is the provenance of Enterprise Risk Management (ERM).

The Genesis of ERM

More than anything else, ERM represents the desire and the will to do a better job of managing risks and an explicit recognition of the short-comings of traditional risk management practices. At its core is an acknowledgement that larger companies require more formalized risk management practices. However, the size and complexity of most large-scale businesses creates an interesting problem – how can companies increase their operational and financial sophistication without compartmentalizing their risk management functions?

The most important tenet of ERM is that risk should be managed for the enterprise as a whole. Managed by operating or functional units, companies tend to misapprehend risk, to make sub-optimal risk financing decisions and to even increase risk by unintentionally making financial and operating decisions that destroy a firm's natural hedges. Therefore, ERM necessitates training management to identify risk issues, to understand all of the ways risk can be managed and to communicate so that all of the firm's risk management initiatives can be coordinated.

While ERM is applicable to all businesses, this concept resonates much more loudly for large, complex organizations with multiple business locations. These companies recognize that they will need the best risk management practices available or they will not be able to protect the wealth they have already achieved or gain competitive advantage in their respective markets.

© MMC Enterprise Risk Management, September 27, 2001

ERM to Date

Most large companies are still coming to grips with the concept of ERM and have not yet gone beyond tactical solutions to managing specific risks. Many companies are intrigued by ERM but are disappointed to learn that it is not a magical solution to the issues of risk management. To date, most ERM efforts have fallen short of their objectives because the people involved started with limited perspectives about what risk is, how it affects the different parts of a company, and how it can be managed.

Thus, people with an auditing background tend to think of risk as a financial control issue; those with insurance expertise tend to focus on insurable risk; process experts think reengineering is the answer; actuaries and statisticians prefer to try and quantify risk; strategists focus on business redesign; software engineers think software is the solution to risk issues; and finance experts tend to think first and foremost about transferring risk to the capital markets. Each perspective is valid in a limited way but fails to fully address all of the risk management issues a company faces. Unfortunately, the limited perspectives of its practitioners have sidetracked many risk management initiatives and have given rise to a number of fallacies about ERM.

Fallacy #1 – Traditional risk management did not work.

Originally the risk management function involved purchasing insurance. Although it was effective in discharging this responsibility, the name of the function implied a much larger role than was typically played. With each hard market, there was a renewed awareness of how limited the risk manager's role actually was. Every time insurance rates increased dramatically, it became obvious that insurance was merely a financing mechanism and that risk management required a variety of financial, operational, and organizational initiatives working in concert to be truly effective.

Recently, a large number of high profile corporate disasters have made it evident that there are many types of risk that are not insurable. This has resulted in a desire to expand the role of the risk management function still further. Some people have naively suggested that the risk management function is responsible for everything that can go wrong in a company.

Aside from making the chief risk officer a convenient scapegoat, this trivializes the importance of other operating and financial managers who are involved in the risk management process. It is also irksome to managers who recognize the limits of centralized control and resent additional constraints being placed on them by "corporate" decision-makers. Risk management is a job that is too big for any one person, and it is obvious that most risks are best managed at their source, by the business unit where it originates. Thus, information sharing and coordination are much more important in fulfilling ERM's objectives than are issues pertaining to control.

Fallacy #2 - ERM is a risk transfer product that combines different types of risks.
Where it is feasible, analyzing disparate risks in concert is useful to determine the most advantageous portfolio of risks and conversely, what risks should be transferred to help produce earnings and cash flow stability. However, some people have used modern portfolio theory to suggest that one can get cheaper coverage by bundling risks prior to transfer. While it is true that an individual risk may be more volatile than a bundle of risks, this does not necessarily make a bundle of risks more desirable.

Ultimately, the cost of risk is determined by the preferences of the risk taker. Assuming that there are no blanket institutional prohibitions against a particular type of risk, a given risk will be more or less desirable based on the impact that it has on the risk taker's portfolio. Thus, the price will be based largely on how efficiently and widely risk can be distributed. It is the job of a company's financial managers in concert with their (re)insurance broker to determine how to achieve the most cost-effective distribution of risk.

Fallacy #3 – Reengineering eliminates most risk issues.
Reengineering tends to be a massive undertaking to realign and reposition an enterprise for maximum efficiency given current business conditions. While process redesign may improve competitiveness, it is not very useful for risk management. Most companies already have a full complement of techniques for dealing with known risks. Since reengineering is a reactive strategy, it is not very helpful for identifying when conditions change and when new risk management strategies are warranted.

Fallacy #4 – Software is key to solving risk issues.
Poor communications about risk and risk management are one of the greatest roadblocks to ERM. Nevertheless, installation of a new computer system that permits data warehousing, statistical analysis, and comparison of best practices will not solve this problem. By itself, software does not help identify new risk issues or determine the most appropriate ways of managing them. Furthermore, the time and money necessary to create such a system and to train people to use it can be a huge distraction. Implementing such as system before managers have a thorough knowledge of risk and risk management is truly putting the cart before the horse.

Fallacy #5 – Risk identification is easy.
Most companies use their resources to ensure that the things that have gone wrong in the past never happen again. This works well for the particular manifestations of risk that they already know about but does nothing to uncover emerging risk issues. Thus, companies often think that they have an effective approach to handling a risk issue, when in fact, they have only dealt with one manifestation of that risk issue.

Companies must supplement their experienced-based approach to risk management with an environmental approach. Rather than just looking at the past, managers must look carefully and systematically at their companies in the context of their present environments. The external environment is constantly changing and companies must continually reassess how they respond to those changes. They must ask themselves how their companies create and store value and what threatens the value creation process.

Fallacy #6 – Risks must be classified.

Some people believe that risk classification is an important step in the risk management process, and they use many different risk classification schemes to accomplish this objective. For example, risk may be characterized as operational, hazard, financial, or strategic. However, risk is never quite so delineated as these schemes would suggest. Perhaps a risk, such as fire, begins in the hazard category. However, it does not take much imagination to see how this risk issue can quickly engulf the operational, financial and strategic aspects of a business as well. Aside from being an unnecessary step in the risk management process, risk classification schemes may implicitly suggest that risks can be partitioned among the enterprise's managers, when, in fact, risk management is every manager's business.

Fallacy #7 – Risks must be quantified.

That it is worthwhile and meaningful to attempt to quantify every risk is one of the most glaring fallacies of ERM.   If one could just measure all risks and put them in a common framework, the thinking goes, one could invent all sorts of new risk transfer instruments. In fact, we deal effectively with most risks every day without quantifying them.

The real value of risk assessment is for allocating risk management resources and determining when risk transfer is worthwhile. Nevertheless, most risks can be managed with so little resource that it is not worth trying to measure them.

Aside from poor data quality and insufficient experience, most companies' risks are not measurable with any degree of certainty because they are not distinct in their own right or separable from management action. For these same reasons, risk can be difficult or impossible to transfer without using traditional financial means such as issuance of debt and equity, where all the net risks of a firm are bundled together.

Fallacies #8 - There are consulting firms that do ERM.

ERM is not a project. It is a process that companies embed in their organizations to continuously monitor their companies and their environments to determine the best ways of dealing with risk issues. An ERM process requires a detailed knowledge of every nook and cranny of a company and its environment as they evolve over time. ERM requires multi-faceted and varied expertise that only the company's management team would possess.

A consulting firm can provide an independent and objective view of an organization and can help teach managers how to implement an ERM process, but the company has to take responsibility for making this process work. A good consultant can challenge a company's risk management processes and thinking, but she cannot possibly understand the company they way its managers do. In short, ERM is a full-time job that must be done by the company's own managers.

Fallacy #9 - Risks must be prioritized.

Having identified many potential manifestations of risk that might affect the company, a company's ERM team and its consultants are often overwhelmed and seek to identify the "really important" risk issues. This puts the ERM team in the awkward position of having to dismiss the overwhelming majority of the risk issues that management identified as being important. The real problem is that the combined ERM team does not have the knowledge or resources to address more than a few risk issues. Even then, they can only address these issues in a limited, high-level way. This would not be an issue if they could really harness all the functional strengths of the company. After all, large companies manage countless risk issues everyday.

Equally important is the difficulty that most people have in distinguishing between a particular manifestation of risk and the underlying risk issue. Most organizations have relatively few risk issues, but these issues manifest in countless ways across the enterprise. Identifying particular things that can go wrong is not worthwhile because one cannot possibly imagine them all and one cannot manage them without first understanding the factors underlying each risk issue. For example, there are countless ways that credit risk can manifest but underlying each instance is an obligation from another party. In order to manage credit risk, a company must understand its relationships and consider how it can eliminate, minimize, transfer, or otherwise protect against potential credit losses.

Fallacy #10 - ERM is about using specific risk management tools.

"If you have a hammer, you'll find a nail." This is another way of saying that we should focus our attention on the work and not the tools. ERM is about building a process for risk identification, assessment and management. In each phase of this work, there are various tools and techniques that may be appropriate for a given risk issue. However, the overarching tool is the process itself. At its core, a successful ERM process is about:

- Training people to identify risk issues;
- Teaching people how to assess risks and risk management initiatives;
- Creating an understanding of all the different ways risk can be managed;
- Fostering information capture, transmittal and transparency;
- Documenting assumptions so that they can be reassessed periodically; and
- Organizing people with different skills, knowledge, and functional responsibilities to continuously reevaluate risk identification and management.

Just as there are countless manifestations of risk, there are countless tools that might be used in managing risk. Nevertheless, one needs to have the expertise to know when and how to employ these tools. Before any meaningful consideration can be given to which tools may be appropriate, it is important to understand the business, its environment and its organizational structure. The tool itself is not important without a context and an objective.

The Future of ERM

As these popular misconceptions suggest, a successful ERM process is dependent on having many people with different backgrounds and expertise actively engaged in managing risk. However before this is possible, managers must have a common understanding of how their companies create and store value and the broad, thematic risks that can threaten their work.

Risk management efforts can only be coordinated when there is a full appreciation of how company-wide risks may affect different parts of the enterprise. Once it is clear which operating areas are subject to which types of risk, it is important to consider how each business environment can monitor risk and document current and potential risk mitigation initiatives.

By actively taking steps to identify, assess and manage risk, a company can improve its risk/return profile. ERM helps focus attention on risks that have been previously under-managed and enables a better allocation of risk management resources. From a preventative standpoint, ERM's greatest benefit is the development of an ability to anticipate and prepare for risk issues before they vitiate a company's value proposition. Earnings volatility is diminished along with the capital required to support the enterprise.

In essence, ERM is about coordinating risk management practices over time, across operational and financial dimensions, and across departments and business units. This is sensible and commonplace, and one might say that it is just part of good management, but it is rarely practiced in any comprehensive way. Consequently, it is all too common for companies to discover an operating or financial problem after it has already hit their bottom-line or adversely impacted enterprise value.

This article was published in Best's Review in February of 2002 as "Revealing the Wrongs."

© MMC Enterprise Risk Management, September 27, 2001