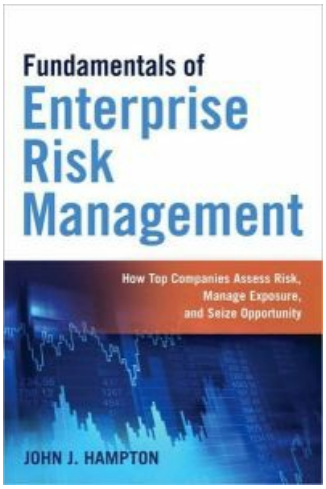

Book Fundamentals of Enterprise Risk Management

John J. Hampton
AMACOM, 2009
Listen now

- play
- pause

00:00
00:00

Recommendation

Fully managing enterprise risk means more than insuring against fire, floods and other hazards. Companies commonly have many uninsured exposures to loss from tougher competition, rapid technological change, financial instability and regulatory sanctions. That is why business leaders in growing numbers have adopted enterprise risk management (ERM), a flexible way to identify and respond to a corporation's total range of risks. Not all risks are all bad. Some are worth taking. Firms that practice enterprise risk management can minimize their potential peril while taking their best calculated risks, the ones most likely to increase sales and profits. Enterprise risk management will not eliminate risk. It did not prevent the failures of major financial institutions during the 2008 crisis. But author John J. Hampton cogently upholds the practice, noting that a disciplined, detailed approach is critical to making ERM actually work. He favors a customizable model of risk management – including a central monitoring function – that can work for a company of any size. *BooksInShort* recommends this book to business leaders seeking a more reliable way to identify each meaningful risk, to distinguish good risks from bad ones and to cover their downsides as much as possible.

Take-Aways

- Enterprise risk management (ERM) is a comprehensive method for dealing with business uncertainty.
- Companies that correctly practice ERM distinguish promising risks from perilous ones.
- Firms must customize their ERM programs. No one approach works for every company.
- An effective ERM system designates an individual or group "central risk monitor" and assigns personnel to handle specific risks.
- Companies should routinely scan their environment for new and emerging risks and opportunities.
- Software for ERM applications can make related risks easier to assess.
- The design of an ERM system should align with your company's business model and fit its overall culture and its subcultures.
- Highly quantitative ERM systems may draw too much attention to probable events.
- Yet improbable events deserve special attention if they could produce dramatic results.
- Certain types of business threats require a team approach to risk management.

Summary

Looking Beyond Insurance to Risk Management

Starting in the 1970s, companies expanded their risk management umbrella from insuring against hazards to launching internal loss-control initiatives, such as safety improvements at assembly plants to reduce workplace accidents. Some companies started to substitute the broader corporate title of risk manager for the older title of insurance manager. In subsequent years, business leaders have gradually put more attention on enterprise risk – not individual risks in isolation, but rather a company's total, embedded exposure to uncertainty. By the late 1990s, some major corporations had started to conduct enterprise risk management (ERM) through regular reassessments of identified risks, routine scans for ill-defined threats and constant analysis of commercial possibilities that held more positive potential than negative.

> "Enterprise risk varies with the line of business, the nature of the entity, political and economic issues, and other factors."

Modern risk management covers mitigating the risk of physical hazards, complying with government regulations, and maintaining productive internal controls and audits. Even given these common ingredients, effective ERM systems come in a variety of different flavors. Therefore, the best way to manage enterprise risk varies from firm to firm. Handling the endless assortment of risks in the business world is one of ERM's greatest challenges. Even within the same industry, no single risk-control formula works for every company. Consider the risk profile of passenger airline JetBlue. Its New York base means that its weather-related risks are not the same as those of airlines centered in the southern U.S. or other temperate zones. In 2007, JetBlue was unprepared for the severe winter storm that halted its flight operations at the hub of its route network, John F. Kennedy International Airport. Many people boarded its planes, but never flew anywhere; they were stranded for hours on the ground because JetBlue had failed to plan properly for the vagaries of winter weather.

How to Approach Enterprise Risk Management

To determine which risks to accommodate and which ones to avoid, a company must designate an internal monitor, either a group or an individual, to perform the "central risk function." This job involves identifying and assessing all the risks the company faces. The internal monitor communicates material findings to corporate managers and to the people assigned to assay specific risks in their areas of expertise. To gain synergy, design and implement an ERM system that aligns with your firm's existing division of managerial tasks, so it blends into the business instead of burdening its managers with substantial new demands. A manufacturer, for instance, would be alert to risks in the areas of "production, marketing, finance, technology, administration, business units" and "key initiatives." In such a company, for example, a "chief production officer" might be charged with managing risks due to "design, supply, process" and "efficiency."

> "Organizations must implement ERM to prove its value, but management often expects the value to be proven prior to implementation."

Effective ERM also must adopt information technology that brings the clout of computer power to complex risk analysis. Structure your ERM system to use the same procedure to assess all risks and to ensure accountability among designated personnel for the way they manage particular risks. For ERM to work, the board of directors must take an active leadership role in the process of risk recognition and management.

Unforeseen Risk and False Optimism

While some risks are predictable, others remain unforeseen until their consequences reveal them. Nassim Nicholas Taleb's influential 2007 book, *The Black Swan*, discusses big, unexpected surprises. Taleb wrote that some events are so shocking and so intense that they are initially inexplicable. The September 11, 2001, terrorist attacks are an example of a "black swan" event, something that happened beyond the boundaries of popular expectations. (Europeans once believed that all swans were white, hence the book's title.)

> "External risks are largely uncontrollable, as they arise from the competitive environment, economic factors, acts of regulatory bodies and other outside sources."

Taleb contended that enterprise risk management is more of an art than a science. He correctly criticized excessively quantitative ERM systems. Too many approaches to ERM put undue attention on what is likely to happen 95 times out of 100 and overlook the potentially dramatic consequences of events that have a 5% probability. Taleb also made an important contribution to ERM by assailing overreliance on factual information about risk, especially historical data. This mistake can contribute to a false belief among company leaders and managers that they understand dynamic, largely random events that defy comprehension. Unchecked, a common human tendency to express optimism in the face of uncertainty can put individuals, organizations and entire societies at great risk.

> "A graphic presentation of risk in a hierarchical structure significantly enhances our understanding of enterprise risks and their relationships."

Some prognosticators foresaw the U.S. mortgage market collapse that led to the global financial panic of 2008. But few correctly predicted the depth of the crisis or the breadth of the resulting scarcity of credit. This is evidence that black swans spotted from a distance become surprisingly larger as they approach. Of course, savvy risk managers consider the impact of probable events, but they also factor in unlikely events that nevertheless would have major consequences.

Software for ERM Applications

Larger companies usually install information technology to support ERM before implementing it. Some ERM software programs create a visual display of risks on the computer screen as an aid to monitoring and prioritization. Managers can use such software to help them determine whether a company's various risks have the potential to interact, and whether designated personnel are mitigating specific exposures to loss and documenting their progress.

> "Is risk management an art or a science? Taleb says it is an art because execution is involved. We can replicate scientific efforts. Risk management varies with each challenge."

Software supportive of ERM allows users to separate their risks visually into main categories with subcategories, which helps people comprehend the interrelationships among different risks. For example, if a company identifies financial instability as one of its main risks, it might show subcategories of risks that could contribute to such instability, including risks related to revenue generation, credit availability, legal actions and regulatory compliance. Companies exposed to a large number of risks can use an ERM software feature called "tagging" to perform complex risk analysis. Tagging allows the user to identify related risks and to analyze them in isolation from other risks. This feature helps users monitor external risks beyond the company's control and assess their potential internal impact.

Five Risks That Call for a Team Approach

Even without a major investment in technology, companies large or small can benefit from a fundamental understanding of certain risks. While many different types of business risk exist, the most common ones include risks related to strategy, leadership quality, company subculture, the age of the company and risk detection. The need for a team approach to these business risks distinguishes them from other risks. No one person can effectively handle any of these five risks:

1. "**Strategic risk**" – A strategic risk taken with purpose and planning can make money. Unknowingly allowing a hidden exposure to fester can be fatal to a company. This is why the central risk function of a well-designed ERM system has "a role in the development and vetting of corporate strategies." ERM emphasizes scanning for trouble wherever it may appear. U.S. manufacturers, for example, should be scanning for strategic threats in China, India and other emerging nations, where companies can make competitive products at lower cost.
2. "**Leadership risk**" – Firms engaged in ERM need to assess personnel risks at the executive level. Leaders make decisions by relying on a mix of assumptions, opinions and feelings, plus provable facts and even mere beliefs. Managers play a different role. They execute leaders' decisions, so firms need strong leaders, as well as solid managers, to detect and defuse the business risks with the costliest potential outcomes, even if they are remote.
3. "**Subculture risk**" – Some companies carry the burden of destructive subcultures. This risk emerges when employees in certain departments adopt divisive attitudes that could impede the progress of the entire firm. Some large companies, in particular, harbor bureaucratic business units with the capacity to subvert management. Organizations must take advantage of the ability to "customize ERM to fit their individual cultures."
4. "**Business cycle risk**" – From birth to death, most companies are subject to a life cycle with a series of stages starting with the business's launch phase, followed by successive periods of growth, maturation and decline. Problems may ensue if leaders fail to adopt policies appropriate to the age of the company. For example, they could apply a mismatched growth strategy to a maturing business.
5. "**Horizon risk**" – Some companies look for risks in close proximity, but fail to inspect the farthest horizons of probability. Minimize this risk by scanning for three types of risks: possible weaknesses due to faulty business models, scarce supplies of critical resources and unfavorable actions by your customers or competitors.

The Dynamic Risk Landscape

Risks constantly change in size and shape. Some established risks decrease in importance as new ones appear. The emergence of the internet permits new types of misbehavior that expose companies to harm, including malicious hacking into business computer systems and the spread of malevolent viruses. The 9/11 attacks firmly established security-risk mitigation as a top governmental and commercial priority.

> "Maybe the biggest strategic risk involves our reliance on fossil fuel."

Regulatory changes also have altered the risk landscape. The Sarbanes-Oxley Act of 2002, for example, requires chief executive officers of many public companies to sign statements attesting to the integrity of their corporation's internal controls and to file these statements quarterly with the U.S. Securities and Exchange Commission. Now, any CEO who loses his or her grasp of internal controls is at risk of both termination and prosecution.

> "ERM scans internally to ensure that managers are located in areas where stability is needed and that leaders are situated in areas where change is needed."

The global financial crisis of 2008 frightened companies into redoubling their efforts to guard against credit scarcity and financial insolvency. Except for an apparent decline in the chance of a nuclear war between the United States and another country, the world may be accumulating – not subtracting – risks that threaten business interests.

More Leaders Than Followers?

Leading practitioners of enterprise risk management provide standout examples of how it can help companies improve their overall performance. One is Paul Buckley. He had a 29-year career in telecommunications, and he developed a managerial specialty in risk control. He went from the telecom industry to industrial conglomerate Tyco International, which hired him as vice president of risk management. Among other improvements, he broadened Tyco's system of risk control and converted risk advisers at the company into operational staff, making them responsible for executing specific elements of the company's ERM program.

> "A missed opportunity is usually more of a risk than a business disruption."

Lance Ewing got his professional start in the insurance industry, calculating the risk of accidents at sawmill operations and trucking firms, and in other dangerous lines of business. His occupational focus shifted to loss control and prevention. After a five-year tenure in the insurance business, Ewing took over risk management in the public school system in Philadelphia, Pennsylvania. There, his loss-control results produced big cuts in the insurance premiums the public school system was paying. He went on to become vice president of risk management at Harrah's Entertainment, a leading company in the casino gambling industry.

> "ERM drives compliance. Compliance does not drive risk management."

But the ERM field may have more leaders than followers. In 2008, a survey of U.S. corporate executives on the subject of enterprise risk management showed that only 7% of their companies had fully implemented an ERM system, and 33% had no plans to do so. Better management of risk is widely warranted. U.S. companies have paid more attention to regulatory compliance since the enactment of the Sarbanes-Oxley Act. However, compliance is no substitute for proactive identification and management of all the major risks contemporary companies face.

About the Author

John J. Hampton is professor of business and director of graduate business programs at St. Peter's College. He is a former executive director of the Risk and Insurance Management Society.