PRACTICAL GUIDANCE: SEVEN STEPS FOR EFFECTIVE ENTERPRISE RISK MANAGEMENT

WHITEPAPER

THOMSON REUTERS

CONTENTS

INTRODUCTION

Managing enterprise risk in a consistent, efficient, sustainable manner has become a critical boardroom priority as CEOs, CFOs, and other members of the senior leadership team face unprecedented levels of business complexity, changing geopolitical threats, new regulations and legislation, and increasing shareholder demands.

In recent years, external factors have fueled a heightened corporate interest in enterprise risk management. Industry and government regulatory bodies, as well as investors, have begun to scrutinize companies' risk-management policies and procedures. In an increasing number of industries, boards of directors are required to review and report on the adequacy of risk-management processes in the organizations they administer.

The reason for the increased interest is simple. Virtually all of the risk events impacting corporations today are foreseeable and manageable. Virtually none are truly random and unpredictable. It is the responsibility of directors and senior executives to ensure that avoidable losses are consciously managed. Not so long ago, risk management was considered a niche specialty, the province of academics and consultants, and not a priority for mainstream businesses.

For many firms, the investment in enterprise risk management is the direct result of experiencing one or more avoidable significant business failures. For other organizations, the heightened focus on enterprise risk management is the direct result of the Sarbanes-Oxley Act or recent changes to SEC proxy disclosure rules which place greater responsibility on the board of directors for understanding and managing an organization's risks.

Regardless of the driver, the recognition that business success depends on striking a balance between enhancing profits and managing risk and the investment in the discipline of enterprise risk management is now top of mind for most business leaders.

DEFINING ENTERPRISE RISK MANAGEMENT

Enterprise risk management is sometimes viewed as a way of aggregating, managing and reporting on all of the risks facing an organization – a way to consolidate the information within the individual risk silos. That is a necessary and desirable goal, but it is not specifically enterprise risk management. While there are many different definitions of enterprise risk management, many organizations have standardized on the definition outlined in COSO's *Enterprise Risk Management—Integrated Framework*, published in 2004.

Enterprise risk management is defined by COSO as a process designed to:

1. Identify potential events that may affect the organization
2. Manage risk to be within the organization's risk appetite
3. Provide reasonable assurance regarding the achievement of the organization's objectives

The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed.

The COSO definition goes on to outline eight interrelated components of enterprise risk management. These disciplines are derived from the way management runs an enterprise and are integrated with the management process. These components are:

INTERNAL ENVIRONMENT: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an organization's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

OBJECTIVE SETTING: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the organization's mission and are consistent with its risk appetite.

EVENT IDENTIFICATION: Internal and external events affecting achievement of an organization's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

RISK ASSESSMENT: Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

RISK RESPONSE: Management selects risk responses – avoiding, accepting, reducing or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

CONTROL ACTIVITIES: Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

INFORMATION AND COMMUNICATION: Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

MONITORING: The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

In practice, enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

IF IT'S SO GOOD WHY ISN'T EVERYONE DOING IT?

Value is added by seeking and exploiting opportunities, improving business performance and preventing avoidable loss events.

Enterprise risk management has been promoted for years as an important activity. Boards insist they want more information on enterprise risk, but examples of successful enterprise risk management implementations — sustained over time and across all business functions — are elusive.

Unfortunately, examples of enterprise risk management failures abound. Most of those failures occur when risk management initiatives are conducted in silos and for defensive purposes. While they may, at best, have identified hazards, prevented value erosion and reduced compliance violations, they have often failed to anticipate and prevent catastrophic loss events and have seldom added real economic value. Value is added by seeking and exploiting opportunities, improving business performance and preventing avoidable loss events.

Developing a comprehensive business case for entity wide risk management is difficult. According to the *Global Risk Management Survey: Fifth Edition—Accelerating Risk Management Practices*, published by Deloitte in March 2007, when organizations were asked to rate challenges, "issues surrounding data, culture, tools and supporting technology/systems were rated most often as very significant."

Many organizations found it difficult to create a solid business case for enterprise risk management, in part due to the difficulties of quantifying the full range of benefits. According to the study, "...only 13 percent of executives said that their firms quantify enterprise risk management costs and just 4 percent said they quantify enterprise risk management value." An estimate of the human resources, technology and corporate energy investment required to fully implement risk management across an organization is elusive.

Most business cases for comprehensive risk management focus on cost savings and efficiencies and fail to make a compelling case for adding value. Successful enterprise risk management adds value by avoiding losses. That is a hard case to make and prove.

Perhaps the biggest driver of enterprise risk management will be the emergence of corporate responsibility or sustainability reporting. Sustainability is defined as meeting the needs of the present without compromising future generations. Proponents argue that traditional governance, risk and compliance activities cover only about 20 percent of the information that management and stakeholders require.

In other words, what enterprise risk management should ensure is sustainability of the enterprise by addressing risks impacting all the key areas where sustainability is essential.

1. Economic performance
2. Environmental performance
3. Labor practices and performance
4. Human rights practices and performance
5. Social responsibility
6. Product responsibility

Enterprise risk management must continue to address risks and opportunities at the strategic level.

FROM RISK TO OPPORTUNITY

Enterprise risk management must continue to address risks and opportunities at the strategic level. The strategic risks that companies face can be classified into seven broad categories. This following list from *Rotman* – The magazine of the Rotman School of Management, is not inclusive but it represents a good starting point and categorization scheme.

STRATEGIC RISK	COUNTERMEASURE
Industry margin squeeze	Shift the compete/collaborate ratio (Seek collaboration opportunities – sharing back office functions, co-production, asset sharing etc.)
Technology shift	Double bet (Invest in two or more versions of a technology simultaneously).
Brand erosion	Redefine the scope of brand investment Reallocate brand investment
One of a kind competitor	Create a new, non-overlapping business design (Establish a position in an adjacent space)
Customer priority shift	Create and analyze proprietary information Conduct quick and cheap market experiments
New project failure	Engage in smart sequencing Develop excess options Employ the stepping stone method
Market stagnation	Generate "demand innovation" (Redefining the market by looking at it through the lens of customer economics)

Countering the Biggest Risk of All, by Adrian Slywotzky and John Drzik*Rotman* – The magazine of the Rotman School of Management at the University of Toronto, Spring 2007

Within the existing silos of risk management in an entity, such as audit, compliance, IT governance and financial management, the concept of risks as threats predominates, and the result is a focus on controls that prevent or minimize the threat.

Enterprise risk management must focus on opportunities and provide insight into overcoming obstacles to realizing those opportunities on both a strategic and tactical level.

WHO SHOULD BE IN CHARGE?

In 2001 The Institute of Internal Auditors Research Foundation published a comprehensive survey titled, *Enterprise Risk Management: Emerging Trends and Practices*. The survey, based primarily on financial services, energy, and mining industry responses, suggested that senior executives were most likely to oversee an enterprise risk management process. For organizations with existing enterprise risk management processes, chief audit executives, chief financial officers and chief risk officers dominated the leadership statistics.

More recent reports suggest enterprise risk management leadership should remain at the top. In their recent *Guide to Enterprise Risk Management: Frequently Asked Questions*, Protiviti makes the point that the participation, if not the leadership of the CEO, is essential to keep the focus at a strategic level.

Enterprise risk management must focus on opportunities and provide insight into overcoming obstacles to realizing those opportunities on both a strategic and tactical level.

SEVEN STEPS TO EFFECTIVE ENTERPRISE RISK MANAGEMENT

STEP 1: MANAGEMENT'S ROLE

Management's role, often executed in a structured workshop setting, is to engage in risk assessment and prioritization through purely qualitative assessment and "gut feel" based on experience. Although simpler, the results must stand up to scrutiny from knowledgeable experts and experienced practitioners.

Qualitative screening of risks is also useful in making an initial assessment of the level of risk. More detailed quantitative analysis may follow. Management must ensure that the initial risk identification and assessment is comprehensive and balanced between internal and external sources of risk. The focus must be on anticipating strategic and emerging events.

STEP 2: ESTABLISH THE CONTEXT

Enterprise risk management begins with establishing the context of the risk assessment. In the risk management literature, the "context" is commonly thought of as the opportunity, strategy, outcome or process on which stakeholders want formal analysis and assurance. AS/NZS 4360: 2004, a widely accepted risk management standard published by Standards Australia, suggests that the strategic context, the organizational context, and the risk management context must all be considered.

The assessment of the strategic context links the organization's mission and strategic objectives to the management of risks to which it is exposed. Defining the risk management context involves setting the scope and boundaries of the risk assessment process, including the time frame and specific project or activity.

A context could include the entity as a whole, a business unit, a line of business, a major business process, a geographic area or all of the above. The context is the level at which management feels the need to set strategy and assess risk. And, the contexts defined for risk assessment must reflect the economic value of the organization and the business model for creating value. The goal is to simplify and clarify the complexity of the business, not to replicate it.

Whatever the context, it will usually be the basis for formal board reporting and will usually include a variety of existing business activities and functions. Whatever the context identified for an enterprise risk management assessment, it must be sufficiently important to be visible to the senior officers and the board. Its importance may be due to its current significance or its potential significance. The entity's entire portfolio of economic assets should be considered.

A simple but effective way to get started is to establish the initial context as the company's major geographic areas, business units or product lines. These are the focus of management's strategic initiatives. The emphasis is on steering the organization toward value adding opportunities.

STEP 3: IDENTIFY AND PRIORITIZE ENTERPRISE RISKS/EVENTS

The goal of risk or event identification is to produce a list of risks or events categorized into each of the seven areas described in Figure 1. Risks in this context are potential events that, if they occur, will adversely affect the ability of the entity to achieve its objectives. By definition, managing risks is necessary to achieve the organization's strategies and objectives. The way in which risks are managed will affect the value they add and provide competitive advantage. Some events may have a positive impact. These represent opportunities.

A simple but effective way to get started is to establish the initial context as the company's major geographic areas, business units or product lines.

In the struggling airline industry, one of the biggest risks is excess capacity, operating costs and the squeeze on margins. Some independent airlines have turned cost risk to a competitive advantage by minimizing fleet diversity, maximizing aircraft utilization and reducing turnaround times.

Completeness in risk or event identification is critical. Risks and events left unidentified are excluded from further analysis. Unidentified risks represent unidentified opportunities. Strategic risks should be explicitly identified even (and some would say especially) if they are apparently outside the control of the entity.

For the risks or events identified, management should consider the severity, the probability and the impact of time on the event. When will the event occur? When will it disappear? What is the rate of change in severity and probability? What is the lowest level in the business where a catastrophic risk could occur? How is that risk managed and reported? Think of an oil and gas company with hundreds of oil and gas wells, dozens of refineries, thousands of miles of pipeline, millions of gallons of petroleum product in transit, or in storage.

STEP 4: CHOOSE TOOLS FOR RISK/EVENT IDENTIFICATION AND ASSESSMENT

ISO 31000 suggests the use of checklists or risk source models to promote consideration of all risks. COSO ERM – Integrated Framework suggests a range of event identification techniques ranging from facilitated workshops with senior management to studies of the use of event category tables.

While quantitative approaches to risk assessment are attractive for their apparent precision, the variables involved in enterprise risk management are seldom sufficiently accurate. Qualitative risk tables are often used to provide a consistent assessment of severity and probability.

STEP 5: DON'T FORGET THE UPSIDE

Consider the potential positive outcomes from events and the impact of risks that do not occur. Enterprise risk management should add value at the strategic level and the value must come from strategic decisions based on a careful analysis of and response to risks and events.

STEP 6: ASSESS HOW EXISTING PROCESSES MITIGATE RISK AND EXPLOIT OPPORTUNITY

Enterprise risk assessment identifies areas where management systems and processes are required to support the achievement of objectives. Linking enterprise risks to the processes or systems that support the management of those risks creates alignment within the organization.

If an assessment of enterprise risk identifies a gap in the management framework, that gap can be addressed more quickly and effectively.

For example, fast growing technology companies may identify delays in product development or poor product quality as significant risk areas. Enterprise risk management connects these risks with the actual processes or organization elements that are accountable for new product development and product quality. The significance of those processes or divisions is then understood and managed in the context of the enterprise risk identified. The value adding potential from timely product development and product quality initiatives are maximized. Conversely, if an assessment of enterprise risk identifies a gap in the management framework, that gap can be addressed more quickly and effectively.

Enterprise risk management may identify raw material shortages as a significant risk. As a result, the company may choose to put processes in place to hedge against future price increases, to seek alternative sources of supply or to redesign products to consume less of the scarce resource.

Finally, enterprise risk management will identify business processes and locations whose value to the business is low or indirect. These processes or organization elements may be streamlined or outsourced and the resources reassigned to more value-added activities.

STEP 7: LINK ENTERPRISE RISK MANAGEMENT TO OVERALL GOVERNANCE, RISK AND COMPLIANCE

Enterprise risk management sits above the elements of integrated governance, risk and compliance but must be linked to them. The common denominator linking enterprise risk management with existing risk silos is the risk-based approach established in the enterprise risk management initiative, including the language, tools and technology for storing and managing the information produced. The organization should have one single framework for managing risk and a common language and tools for implementation across the organization.

Effective operational risk management ensures the tactics necessary to support the strategies are in place and functioning at an acceptable level of risk. Operational risk management focuses on the reliable performance of processes deemed critical to strategy.

Compliance programs are essential to operate within management's discretionary boundaries and the law. More than ever before, business is expected to operate within the boundaries of safety, environmental, supply chain and consumer protection laws that change from one jurisdiction to another.

Financial control management provides assurance that the information management uses to run the business and report to stakeholders is reliable. Stakeholders rely on complete, accurate and timely financial reporting and failures can have an immediate and negative impact on value.

IT governance provides assurance that the technology management relies upon is operating effectively and reliably. Information technology is more than a source of cost savings; it is a source of strategic advantage. Sound IT governance practices are essential to achieving strategic goals.

Audit is an essential element of governance, risk and compliance, and provides assurance and recommendations to management and the board. Audit is relied upon to ensure all the pieces of governance, risk and compliance are working together effectively.

ENTERPRISE RISK MANAGEMENT – ITS TIME HAS COME

Mismanagement of strategic risks has been shown to be a major cause of loss of shareholder value. In the report by the Institute of Management Accountants referred to earlier, *Evolution of Risk Management -Enterprise Risk Management: Frameworks, Elements and Integration*, two studies are cited as analyzing value collapse. One study by Mercer Management Consulting found that 10 percent of the Fortune 1000 lost 25 percent of their value within a one month period. Another study, by Booz Allen Hamilton, suggested that of 1,200 firms with market capitalizations greater than $1 billion, the primary events triggering the loss of shareholder value were strategic and operational failures.

The evidence is compelling that strategic failure can cause enormous, irreversible and sometimes sudden value loss. Are these losses predictable and avoidable? Can strategy be made more resilient by enterprise risk management? Clearly, many companies do avoid strategic failure and thrive in adverse circumstances.

Proving that enterprise risk management will prevent or mitigate strategic failure may be difficult. But the tools for implementing enterprise risk management are readily available, implementation is not complex and the cost is not high compared to the cost of failure. It is easier to argue that the time has come when enterprise risk management should be a standard management practice.

.

The evidence is compelling that strategic failure can cause enormous, irreversible and sometimes sudden value loss.

ABOUT THOMSON REUTERS

Thomson Reuters is the world's leading source of intelligent information for businesses and professionals. The company combines industry expertise with innovative technology to deliver critical information for leading decision-makers in the financial, legal, tax and accounting, scientific and healthcare markets.

Our solutions dynamically connect business transactions, strategy, and operations to the ever-changing regulatory environment, providing highly regulated firms with the knowledge to act. Our client groups include compliance, audit, legal and risk functions within the organization. We partner with firms to manage their risk exposure and accelerate their business at every step.

The Thomson Reuters Accelus™ suite of products provides powerful tools and information that enable proactive insights, dynamic connections, and informed outcomes that drive overall business performance. Thomson Reuters Accelus is the combination of the market-leading solutions provided by the heritage businesses of Complinet, Oden®, Paisley, West's Capitol Watch®, Westlaw® Business, and Westlaw Compliance Advisor®.

Learn More
Call: 763.450.4700
Email: enterprisegrc@thomsonreuters.com
Visit: accelus.thomsonreuters.com

© Thomson Reuters. All rights reserved.
Republication or redistribution of Thomson Reuters content, including by framing or similar means, is prohibited without the prior written consent of Thomson Reuters. 'Thomson Reuters' and the Thomson Reuters logo are registered trademarks and trademarks of Thomson Reuters and its affiliated companies.

Cover image by Reuters.