



Enterprise Risk Management

Complacency Is
No Longer an
Option, But a
Practical Start Is

ADVISORY

AUDIT ■ TAX ■ ADVISORY

© 2006 KPMG International. KPMG International provides no client services and is a Swiss cooperative with which the independent member firms of the KPMG network are affiliated. All rights reserved.



Experience Shows Why ERM Is Critical Now

Business Improvement Imperatives

- Improve financial and operational performance
- Reduce losses
- Enhance competitive advantage

Regulatory Requirements

Organizations are challenged by increasing regulatory requirements to have formalized risk processes in place. They must:

- Satisfy industry mandates, such as energy, banking, health and safety, and insurance regulations
- Satisfy corporate governance requirements (e.g., Sarbanes-Oxley section 404)
- Meet SEC Requirement: 10-K description of “Risk Factors” in plain English
- Meet new NYSE ERM public company listing requirements emphasizing board responsibilities and corporate governance
- Uphold a board’s duty of care in managing a corporate entity

Key Stakeholder Demands

Rating agencies and analysts are increasingly monitoring business assessment of risk. Organizations must:

- Comply with rating agency guidance emphasizing a company’s ability to articulate and execute against a risk management strategy
- Address analysts’ interest in evaluating governance efforts

Enterprise Risk Management: Complacency Is No Longer an Option, But a Practical Start Is

In an environment in which risks are proliferating, shareholders are demanding growth, and first-movers are expanding rapidly into new markets, many leaders recognize that implementing an enterprise risk management (ERM) program is becoming an urgent business priority.

Business imperatives, regulatory requirements, and rating agency monitoring are prompting a new focus on ERM (see box at left). In response to external pressures, many board members are expecting their management teams to implement an effective ERM program. Consequently, many leaders are seeking guidance in developing a practical approach to ERM—an approach that is tailored to their culture and structure, aligned with their business strategy, embedded in their business processes, and focused on their most critical risks.

Getting started with a clear and practical vision is critical, and a few key steps can enable leaders to build on existing risk assessments and get an ERM effort under way. Leaders who have successfully pioneered ERM tend to embrace several important practices, which may help others meet regulatory demands and add business value. Described below, these leading practices can provide the means of overcoming old barriers, achieving new buy-in, and ultimately realizing ERM’s potential for enabling organizations to add business value and achieve competitive advantage.

1. Gain Buy-in from Those Running the Business. Often in the past, ERM was a finance department “bolt-on” project, the champions of which likely had little broad support or leverage. As a result, ERM’s potential value to the business was never fully realized.

A key step now is to establish a management risk committee (or risk council) that is charged with obtaining buy-in for the ERM program across the organization. With a lead/sponsor reporting to the CEO, the risk council would include individuals who lead key areas within operations and support, such as legal, HR, compliance, finance, operations, strategy/corporate development, and IT.

The risk council:

- Assists in educating employees and coordinating development of the risk profile (i.e., prioritized analysis of key risks)
- Confirms and approves the organization’s risk “language” and parameters (e.g., the point at which, for example, something would be considered a catastrophic risk, based on reduced cash flow, loss of operations, loss of reputation, and so forth)
- Sponsors and participates in reviewing the key risks and debating the risk profile, risk priorities, and important risk causes and consequences
- Evaluates emerging risks, discusses and reviews the risk reports, and reports frequently to the CEO and the board
- Facilitates process of keeping risk profile current and relevant

Having obtained consensus, the risk council is in a position to steer the ERM execution effort.

Understanding Risk

When a risk is categorized according to its likelihood and its potential consequence, leaders can determine how it may affect variables including profitability, market share, and reputation. They are then better able to understand and manage the risk, based on whether it is:

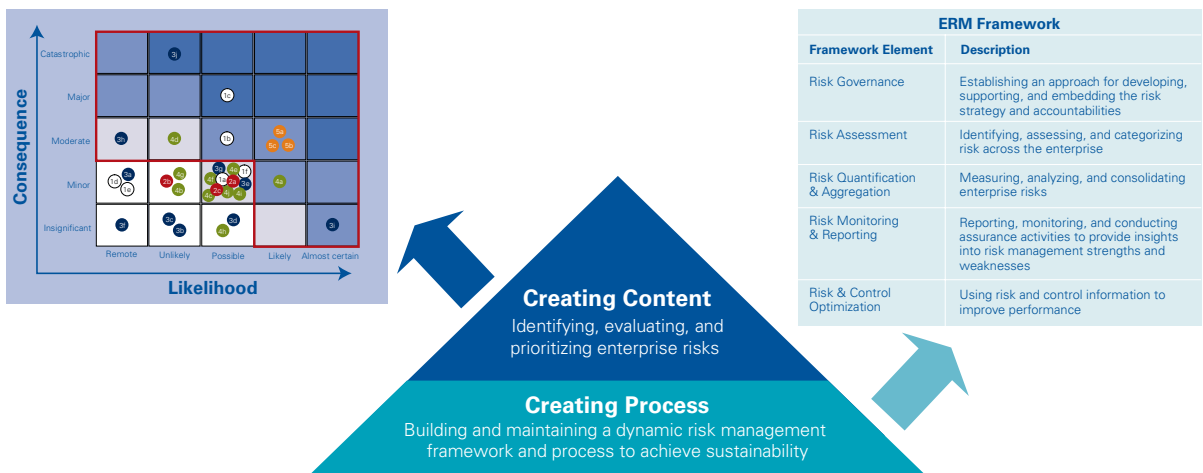
- **Controllable.** A risk occurrence management can reduce or prevent.
- **Uncontrollable.** A risk occurrence that management cannot prevent but that it can detect as well as manage the risk consequence.
- **Discrete.** One-time event that impacts business objectives within a discrete time frame and may recur.
- **Ongoing.** Iterative event that impacts business objectives over an indefinite time frame.

2. Identify and Prioritize Top Risks—and Explore How Well You Manage Them.

A successful ERM endeavor begins with a focus on two fundamentals: content and process (Figure 1). “Content” refers to key risks, and “process” indicates how the program for managing them is sustained across the business. The risk council’s first goal is to facilitate the identification and prioritization of an organization’s key risks—those that may prevent it from meeting its corporate strategic goals. This list can be based on the likelihood of the risks occurring and the potential consequences to the organization should they occur (see box at left). Leaders would identify risks that they believe threaten the business model, the organization’s strategy, and the organization’s existence. Members of management within the risk council would vet these risks, develop an enterprise risk profile, and then identify priority risks (e.g., the top 10 to 20 risks). The risk council’s second goal is to explore how well the business prevents and/or manages the key risks today and what changes may be necessary to improve that effort.

This process provides details about the effectiveness of the organization’s approach to managing risk and an assessment of vulnerabilities that could threaten the organization’s overall business strategy. This process can also assist leadership in critical decision-making. For example, if an organization is planning to buy another company, the relevant risk information could help illuminate whether the potential acquisition could have a negative impact on the company’s current top risks. So much business information is historical; risk information needs to be current and supported by a sustainable process to help enable a future focus.

Figure 1: ERM Fundamentals



Implementing ERM successfully calls for doing two things well: creating content and creating process.

Source: KPMG LLP (U.S.) 2006

3. Assign Accountability: Turning the Corner from Risk Assessment to Risk Management

Management. Identifying key risks will help the organization understand accountability—who owns the risks, how effectively they are currently being managed, and whether the risks are being monitored. Internal audit or compliance departments may be in charge of monitoring certain risks, but often, because organizations are organized by function or geography and not risk, the highest risks may not have designated risk owners or risk monitors. Indeed, some risks may not be formally identified (for example, strategic risk is often not identified, and thus can be the source of some unwelcomed surprises). Assigning formal accountability for identified risks to the right people helps create a greater level of assurance for the board and the audit committee and a greater level of confidence in the organization’s governance framework.

4. Begin Working Toward a Single View of Risk. Many organizations have already invested in a variety of risk processes and functions, but these mechanisms often lack a unifying vision and clear objectives. Consequently, the potential benefits are unrealized. The effective implementation of ERM is the much needed “glue” that delivers a performance-based focus on risk management and, thus, a reward for the risk management investment. Implementing a single ERM approach allows leaders to replace the siloed approach to risk management with a single view of risk that is articulated across the organization.

5. Consider Your Current Position within an ERM Framework. The risk council can then build consensus on where the organization wants to go next, based on its risk profile. With a single view of risk identified and an ERM framework (i.e., a construct of common language and approach/methodology for risk management) in place, an organization can begin the critical work of articulating its own vision for ERM and ERM’s role in the organization. That vision will help determine the organization’s ERM approach and will likely be a call to more immediate action as leaders gain an appreciation of the gaps in their current efforts and can see a way forward.

Leaders take varying approaches to ERM, depending on the needs of the organization and its risks. As outlined in Figure 2, ERM approaches can be plotted along a “maturity continuum.” An organization’s approach, and the choices it reflects, affects the extent to which it makes ERM part of its governance and business operations.

Figure 2: A Risk Continuum

Level	Basic	Mature	Advanced
Approach to ERM	Remain in compliance	Deploy as a management process	Embed as a strategic tool
Goals	The organization has identified its top risks and has prioritized and addressed its compliance risks.	The organization has a process for managing risk and a governance framework that supports the process. It manages compliance risk against strategic goals.	The organization has embedded an ERM process; senior leaders use risk information as the basis for decision making; ERM is linked to performance measurement.

Source: KPMG LLP (U.S.) 2006





The Way Forward

ERM has evolved from a largely theoretical construct to a highly practical performance tool. Now, many leaders are beginning to recognize ERM's value and practical applicability as a means of responding to business or governance changes and stakeholder demands, improving the management of identified risks, and ultimately creating a sustainable process for gaining competitive advantage. Organizations that embrace ERM and build it into the core of their enterprises can anticipate the benefits that are possible when:

- ▼ Risks (the “content”) are assessed, evaluated, and correlated across the enterprise
- ▼ A common risk framework (the “process”) is in place, with accountability established for measuring, managing, and monitoring risk
- ▼ Risk quantification and aggregation is enabled throughout the organization via common methodologies and tools
- ▼ Risk reporting to management and the board is effective (that is, it captures risk trends and emerging risks)
- ▼ The ERM program supports strategic decision making and brand protection and has predictive value
- ▼ Corporate governance processes are strengthened

Implementing an ERM approach is certainly not easy, and it cannot happen overnight. But as ERM's practical applications evolve, leaders have learned that an ERM approach can help organizations with two critical challenges: (1) How to derive tangible value from regulatory compliance efforts and (2) how to link risk and strategy to drive business performance and enhance the organization's brand. Now that complacency is no longer an option, taking the practical first steps to build internal consensus can help enable leaders to meet rising external demands and, over time, to use ERM as the foundation for building competitive advantage.

ERM Helps Enhance Performance and Value

Using ERM, organizations can:

- Reduce cash flow volatility using derivatives, insurance, or improved controls
- Allocate and evaluate capital based on risk-based performance
- Integrate risk and business planning, investment, and M&A
- Reduce costs through risk consolidation and cross-functional efficiencies
- Reduce losses through coordinated enterprise risk monitoring and reporting



KPMG Contacts

National

John Farrell
Partner
U.S. ERM Lead
212-872-3047
johnmichaelfarrell@kpmg.com

Ted Senko
Partner
302-295-8828
tsenko@kpmg.com

Southwest

Michael Wilson
Partner
713-319-2291
michaelwilson@kpmg.com

Midatlantic

Mark Twerdok
Partner
412-232-1599
mtwerdok@kpmg.com

Northeast

Deon Minnaar
Partner
212-872-5634
deonminnaar@kpmg.com

Midwest

William Sacks
Partner
312-316-1466
wsacks@kpmg.com

West

Jim Negus
Partner
213-955-8507
jtnegus@kpmg.com

Southeast

Sergio de La Fe
Partner
305-913-2736
sdelafe@kpmg.com

KPMG contributors to this publication include John Farrell, Jesal Asher, Carole Law, Christina McGrath, and Diane Nardin.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2006 KPMG International. KPMG International is a Swiss cooperative. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. Printed in the U.S.A. AASC017

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

