



## The Business Case for a Risk Executive:

Leading Efforts to Avoid Surprises,  
Maneuver through Challenges,  
and Add Value

KPMG LLP





## Introduction

Robust risk management efforts are increasingly critical in a volatile global economy, when organizations face a growing number of risks that can affect their ability to be competitive and remain a viable entity. With new regulatory and governance requirements on the horizon - the SEC's proposed Disclosure Rules (linking compensation and new Board oversight of risk management) and the impending Shareholder's Bill of Rights (creating a new Board-level risk committee), organizations are under heightened scrutiny to address and assume new responsibilities for risk management.

Before the economic downturn, many organizations believed they had established enterprise risk management (ERM) programs or functions and thus had established the appropriate infrastructure to anticipate and manage risk. In the wake of the evolving crisis, however, as new and unexpected risks emerged, numerous organizations saw they had taken just preliminary steps in an ERM initiative. The focus was on compliance more often than efforts to managing risk across the enterprise.

Many also recognized that their risk management efforts are focused primarily on complying with Board requests or regulations (e.g., 10-K risk disclosures), rather than serving as a strategic tool—a tool that enables the organization to avoid surprises and maneuver through challenges, in turn adding value and supporting business growth.

At the same time, many organizations saw that they lack an integrated process for managing both emerging and high impact/low probability risks. They fight fires effectively after risk events occur, but have yet to focus on the future, anticipate potential scenarios, and consider how the organization should prevent or prepare for these risk events.

ERM manages risk by anticipating and preparing for changes that are acceptable for an organization's ability to meet its strategic goals.

Specifically, many organizations found that they:

- Did not manage strategic risk—thus leaving the business open to challenges that could affect its competitiveness and sustainability;
- Did not know or consistently define, source, and assign ownership for all key risks facing their businesses;
- Were deficient in understanding enterprise-wide how much risk they were willing to take in pursuit of their objectives (that is, they had not quantified the organization's risk appetite);
- Lacked a risk management champion with the authority and support to coordinate and report risk management across the organization and to the Board.

As these issues came to light, so did the increasingly critical need for dedicated risk management leadership. With the economy in recession and risk management efforts under stress and urgently in need of renewal, a risk executive (RE) is an important champion organizations need to repair, restore, and revitalize lagging risk management efforts to get organizational performance back on track. Such a leader—who has the authority, the support from the top, and the capabilities needed to serve current and future risk management needs—can develop and lead a sustainable ERM program that helps the business create value.

ERM is essential because change is constant.



Figure 1

Source: KPMG LLP, 2009

## The Case for a Risk Executive

With the backing of the CEO and Board, the RE establishes governance, policy, and risk management discipline, working with leaders across functional areas and their siloed efforts to manage risk. The RE understands the organization and its industry. His or her key purpose is to help prepare the organization to respond to change and the risks that emerge in changing times, and to turn those efforts into opportunities that benefit the organization (see Figure 1).

While the benefits of having a RE may be clear, a variety of challenges arise when organizations set out to define the role and establish the position (full- or part-time), determine what type of risk governance structure is needed to allow the RE to be most effective, and identify the right person for the role. This paper is intended to help management and the Board understand the critical importance of a risk executive in an organization today. It is also intended to guide leaders as they establish or augment the RE role in their organizations and embark on meaningful change to risk management.





## Why a Risk Executive? Defining the Role

In the volatile environment we face now, organizations need a RE who can manage the ERM effort so that it delivers immediate and long-term benefits across five critical areas:

- **Strategy:** Risk management is critical to every organization's survival. Yet many organizations do not fully consider strategic risk. The RE is responsible for this effort. He or she is accountable for challenging the validity of the organization's strategy and objectives. The RE has the authority to ask the fundamental questions about what the organization is doing and why, and he or she is supported in doing so by those governing the organization (e.g., the CEO or the Board).
- **Expertise:** Today, a company without a risk executive lacks the skills and leadership of a dedicated risk champion who understands risk management, risk appetite, and risk governance. The RE is a partner to the business—a leader who supports the business by making sure the company is taking risk in the right areas and at acceptable levels.
- **Objectivity:** Organizations need to understand all their risks and know they are managing them appropriately. A risk executive should be positioned and empowered by top management and the Board to help ensure that risks are properly identified and escalated so they can be managed across the organization.
- **Integration and Communication:** The RE enables the organization to increase its agility by synthesizing risks, integrating them into one risk environment, and communicating them to leadership and the Board.
- **Sustainability:** A risk executive establishes an integrated (i.e., not siloed) risk structure and ensures that it is sufficiently robust and flexible to meet current and future needs. The RE makes sure the risk owners know their risks and manage them appropriately.

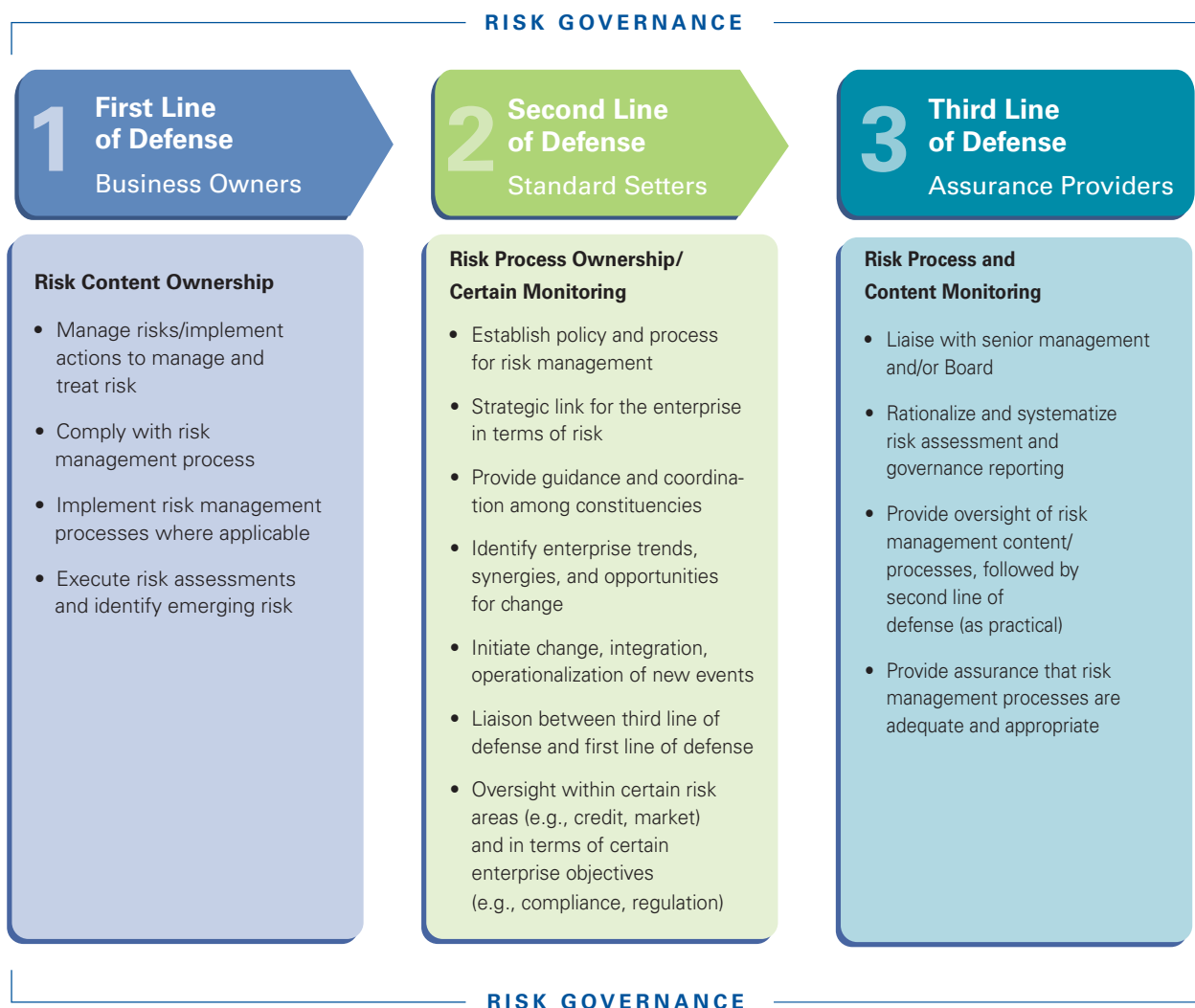
A risk executive can create a new approach to ERM that enables the organization to improve its performance and leverage the benefits that can accrue when one individual, supported from the top, is accountable for risk management. Properly positioned and supported, the RE obtains the quality information needed to facilitate development of a robust risk management organization. Unbiased and able to coordinate conflicting and competing views, he or she can help drive:

1. A complete risk profile, based on a consensus of management, that is used to maneuver and identify new and emerging issues.
2. A heightened risk awareness and structure, which are fundamental to strategic decision making and issues management.
3. A comprehensive system of objective risk limits to assist with the dissemination of acceptable versus unacceptable conditions and scenarios.
4. A robust risk culture, strengthened by the support and guidance of the C-suite and the Board.

## Enabling the Risk Executive: Determining Risk Governance Structure

Led by a risk executive, a lackluster risk management program can evolve into a robust ERM initiative in which three lines of defense provide structure for the holistic management of risks.

### The Three Lines of Defense: A Prospective to Align Roles and Responsibilities in Connection with Risk Management



Source: KPMG LLP, 2009

**Figure 2**

He or she is an independent thinker who can gain the trust and confidence of the C-suite.



Without a risk executive, risk management roles tend to exist in silos, with managers creating policies and procedures for their areas (e.g., Legal, Compliance) and communicating only within those groups. Each business owner tends to manage risks separately within his or her own business unit or functional area. Functional leaders set risk management policies and procedures for their areas, in their silos. Business owners follow those policies and procedures. As a result, assurance providers are left with an impossible task. Each silo is managing risk, but in its own way and only across its area or function. An overall perspective on organizational risk is not possible.

Efforts to address these “disconnects” and create a structured approach to ERM can provide organizations with a new focus on true enterprise-level issues and how they are connected. A risk executive managing ERM would be empowered to establish a common approach and enforce the discipline that allows aggregation, prioritization, quantification, analysis, and reporting of risk at the enterprise level. Across the second line of defense, for example, the RE would be accountable for the use of similar policies enterprise-wide to make sure everyone is thinking about and managing risk in the same way—in every area, function, or business line.

Enabling a risk executive to be successful begins with clarifying responsibilities and accountabilities. While some companies assign direct responsibility for effective risk management to the RE, many others chose to maintain responsibility for risk management with line and functional unit leaders with the RE having important directional, support, and monitoring responsibilities. Companies that have a risk executive position tend to be larger and more complex enterprises. As an alternative to creating the RE position, some companies have assigned this role to a senior officer, such as the chief financial officer, general counsel, chief compliance officer, or treasurer.

Experience shows that success also depends on the RE having the appropriate level within the organization, as well as necessary resources. Some companies provide RE liaisons within subsidiaries, business units, and departments, to ensure RE staff support is close to the entity's operating activities.



## Who is the Risk Executive? Identifying the Right Person

There is no one-size-fits-all RE job description. Every company has its own risk management “signature” requiring different characteristics, skills, culture, and approach. Consequently, the right RE can come from many areas in the organization—including internal audit, finance, other functions, or the business units—as long as he or she has the right skills for the role. Nevertheless, there are some “better practices” to keep in mind when developing the RE’s job responsibilities and qualifications.

The RE has the advantage, and the challenge, of evaluating the organization’s risks enterprise-wide. He or she is accountable for the overall effort as well as for assigning specific risks to others to manage—and then communicating up to senior management and the Board about the steps being taken. He or she can customize and balance the program as the organization matures in its risk management and embeds it in its culture. By focusing on loss prevention (rather than only detection), the RE can help the organization avoid surprises and prepare for emerging risks.

The RE also possesses qualitative capabilities that enable him or her to take the organization’s risk management program to the next level. He or she is a strategic thinker—able to see the big picture and how the organization operates within it. He or she relies on deep institutional and industry knowledge that provides credibility when challenging the status quo. The RE is also an experienced project manager—someone who can facilitate discussion, and gain agreement, among a variety of business constituencies. He or she is an independent thinker who can gain the trust and confidence of the C-suite.

## Next Steps: The RE Agenda

Led by the RE, senior management and the Board can begin to determine steps they should take to augment the organization's risk profile to reflect new and emerging risks, heighten its awareness of the organization's exposure to risk, evaluate risk monitoring, and strengthen its risk culture.

The RE can next set an agenda to advance fundamental conversations with leadership and the Board regarding effective risk management, specifically by seeking the answers to five key questions:

1. Does our existing risk profile accurately capture our risks so we can avoid surprises, given the current state of the economy and the business environment?
2. Do we have the latest tools, techniques, and processes in place to identify and manage our risk exposure?
3. Have we assessed our risk management "culture" to determine whether it is enhancing or detracting from effective risk management?
4. How well are our risk-monitoring functions working?  
Are they operating in tandem or in silos?
5. Are we getting value out of our risk management and monitoring programs and if so, how are we measuring that value?

## Conclusion

Risk management efforts have been tested as never before in the past 18 to 24 months, and many initiatives have fallen short. Governing bodies are seeking new ways to bring Board-level focus to the risk management effort. Leaders are beginning to understand the need to make significant changes, beginning with efforts to establish and support a focused risk executive who can lead a robust ERM program and address important questions about risk profile, exposures, monitoring, and culture. Even if such an individual has other roles in the organization, he or she must be recognized and supported at the highest levels for these vital efforts to own the risk program.

Without a risk executive, risk management efforts will likely continue to lag and hamper the organization's effort to recover. But with a risk executive owning the process, risk management can move beyond a support role and help enable the organization to realize its strategic goals and rebuild business value.



## KPMG Contacts

### Global ERM Lead Partner

**John Farrell**  
212-872-3047  
johnmichaelfarrell@kpmg.com

### Global Risk & Compliance Services Lead Partner

**Mike Nolan**  
713-319-2802  
mjnolan@kpmg.com

### ERM Regional Lead Partners

#### Midatlantic

**Angela Hoon**  
Principal  
267-256-1970  
ahoon@kpmg.com

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

#### Midwest

**Kreg Weigand**  
Partner  
612-305-5581  
kweigand@kpmg.com

#### Northeast

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

#### Southeast

**Kenneth Welch**  
Principal  
404-222-3600  
kwelch@kpmg.com

#### Southwest

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

#### West

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

**Jil Polniak**  
Partner  
650-404-4936  
jpolniak@kpmg.com

Special thanks to the contributors of this Whitepaper: John Farrell, Kreg Weigand, Diane Nardin, Debbie Dacey LoPiccolo, Jennifer Hurson, Nicole Homme and Cynthia Boumann.