



CITIZENSHIP/  
SUSTAINABILITY

DIVERSITY

ECONOMICS

ETHICS

**GOVERNANCE**

HUMAN RESOURCES

LEADERSHIP

MARKETING

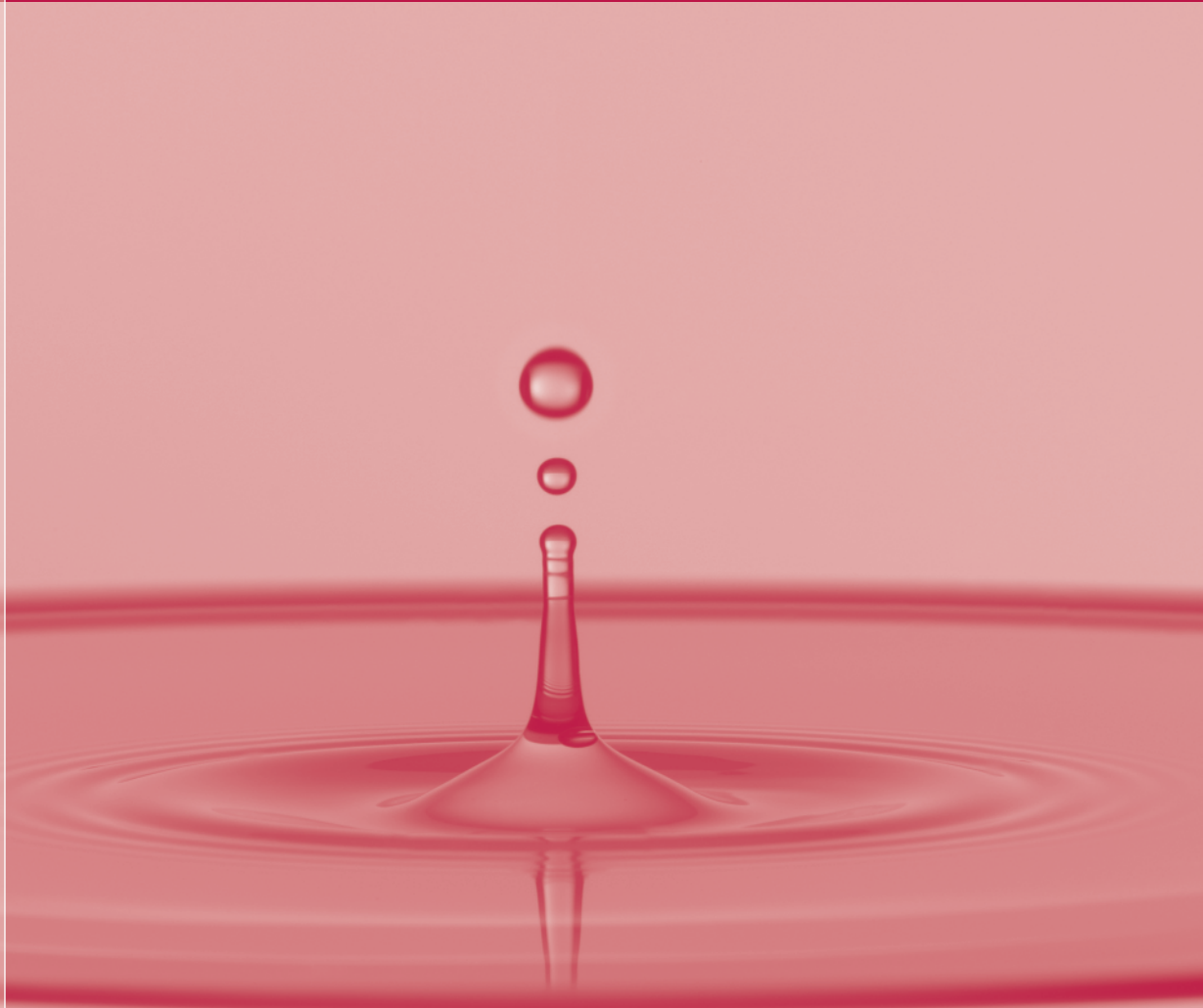
OPERATIONS


RISK MANAGEMENT

# Emerging Governance Practices In Enterprise Risk Management

RESEARCH REPORT R-1398-07-WG

Trusted  
Insights for  
Business  
Worldwide





The Conference Board creates and disseminates knowledge about management and the marketplace to help businesses strengthen their performance and better serve society.

Working as a global, independent membership organization in the public interest, we conduct research, convene conferences, make forecasts, assess trends, publish information and analysis, and bring executives together to learn from one another.

The Conference Board is a not-for-profit organization and holds 501 (c) (3) tax-exempt status in the United States.

## FULL RESEARCH REPORT

### TO OBTAIN THIS RESEARCH REPORT...

**MEMBERS** of The Conference Board can download electronic versions or order printed copies from our Members Only Web site: [www.conference-board.org/ermreport.htm](http://www.conference-board.org/ermreport.htm)

or by contacting Customer Service at 212 339 0345 or via e-mail at [orders@conference-board.org](mailto:orders@conference-board.org)

**NON-MEMBERS** can purchase an electronic version or printed copies at our public Web site, [www.conference-board.org](http://www.conference-board.org) or call customer service at 212 339 0345.

## ABOUT THE REPORT

*Emerging Governance Practices in Enterprise Risk Management* reports on the findings of the Working Group on Enterprise Risk Management instituted by The Conference Board Governance Center in September 2005. Members of the working group met in New York City on September 15 and November 2, 2005, and on January 10, 2006.

Dr. Carolyn K. Brancato is director emeritus of The Conference Board Governance Center. Ellen S. Hexter, C.F.A. served as program chair for the September 15, 2005 and the January 10, 2006 meetings, while Dr. Matteo Tonello was program chair at the November 2, 2005 meeting.

# Emerging Governance Practices In Enterprise Risk Management

by Matteo Tonello, LL.M., Ph.D.

## contents

### 5 Introduction

### 7 Key Findings

### 12 A Top-Down, Strategic, and Holistic Approach to Risk Management

- 12 Elevating Risk Discussions to a Strategic Level
- 16 Cascading the View from the Top
- 17 Capturing Risk across the Enterprise
- 20 Unlocking the Hidden Value of Intangible Assets

### 21 The Legal Foundation of Enterprise Risk Management

- 21 The Expanding Scope of Fiduciary Duties under Delaware Corporate Law
- 22 Federal and Regulatory Requirements
- 24 Securities Exchange Listing Standards
- 24 Federal Sentencing Guidelines
- 25 Risk-Based Capital Adequacy Frameworks in Regulated Industries
- 26 Rating Agency Scrutiny as an External Driver of ERM Implementation

### 30 The ERM Infrastructure

- 31 The Role of the Corporate Board and Its Committees
- 35 The Role of the CEO and Senior Executives
- 40 The Role of Business Unit Managers and Risk Owners

### 43 ERM at Work

- 46 STEP 1: Appreciate the Importance of Enterprise Risk Management
- 47 STEP 2: Assess Gaps and Vulnerabilities in Existing Risk Management Solutions
- 51 STEP 3: Set Underlying Mission and Program Objectives
- 53 STEP 4: Establish the ERM Infrastructure and Assign Leadership
- 58 STEP 5: Compile a Risk Inventory
- 65 STEP 6: Select Assessment Techniques and Define Risk Appetite and Tolerance
- 73 STEP 7: Determine Risk Response Strategies
- 77 STEP 8: Develop Effective Internal Communication and Reporting Protocols
- 80 STEP 9: Monitor ERM Implementation and Execution

### 83 Enhancing Public Disclosure through ERM

- 86 The Enhanced Business Reporting Initiative in the United States

### 91 Conclusion

### 92 The ERM Road Map

## ABOUT THE AUTHOR

**Matteo Tonello, LL.M, Ph.D.**, is senior research associate at The Conference Board Governance Center. A qualified attorney in New York and Italy, he practiced corporate law at Davis Polk & Wardwell from 1998 to 2004.

Recently, Dr. Tonello advised the Italian Commission of Study on Corporate Transparency about the effects of the Sarbanes-Oxley Act on foreign private issuers, and contributed to the drafting of the two final reports by the Commission. A new securities law enacted by the Italian Parliament in December 2005 was largely based on the Commission's findings and related recommendations. Dr. Tonello is the author of two books in Italian on the international convergence of corporate governance standards and the corporate veil piercing doctrine. For The Conference Board, he has authored a report on stock market short-termism and a study of corporate governance best practices in family-controlled corporations. In addition, he co-directed a research project in collaboration with McKinsey&Company and KPMG's Audit Committee Institute on the role of corporate boards of directors in enterprise risk management.

Dr. Tonello received a Master of Laws degree from Harvard Law School and a J.D. from the University of Bologna. He also earned a Ph.D. in Law from the St. Anna Graduate School of the University of Pisa (Italy) and was a Visiting Scholar at Yale Law School in 1997.

## ACKNOWLEDGMENTS

The Conference Board Governance Center and the ERM Working Group members would like to thank Jones Day and the American Institute of Certified Public Accountants (AICPA) for hosting the meetings of the ERM Working Group.

The author is grateful to the following individuals for their comments and contributions in the preparation of this report: Mark S. Beasley, Caryn Bocchino, Carolyn K. Brancato, Carlton J. Charles, George Dallas, Scott Davenport, Bob Eccles, Miles Everson, John Farrell, Rick Funston, Hervé Geny, Tom Graham, Ellen Hexter, Robin Lenna, Janice Lingwood, Amy Pawlicki, Prodyot Samanta, and Janice Wilkins.

In addition, the author would like to thank Katharine Rose Newman for her research assistance.

# Introduction

Rising expectations from stakeholders and a reformed legal environment have put pressure on corporations to assess the quality of their overall response to business risk issues. The sensitivity to risk management is well documented in recent surveys of C-suite executives and corporate directors, who recognize the need to instill process and coherence into an activity that is too often left to the initiative of functional managers or business unit personnel.<sup>1</sup>

The concept of correlating risk management and strategy in an enterprise-wide structure first appeared in the midst of the merger frenzy of the late 1980s. At the time, many executives and strategists acknowledged that the enormous amount of risk undertaken through a series of corporate combinations was not always justified by a sound analysis of long-term prospects. In the 1990s, the debate continued and drew the increasing attention of the business community, only to be partially obfuscated by the more exclusive focus on financial risk resulting from the wave of scandals of the Enron era. A few years into the implementation of the Sarbanes-Oxley Act of 2002, corporations are now ready to leverage their experience with mandatory internal control procedures to establish a more comprehensive enterprise risk management (ERM) infrastructure.

In response to the need for guidance in the design and implementation of ERM, a number of frameworks have been disseminated or are being developed. The most widely known of these frameworks—COSO’s *Enterprise Risk Management—Integrated Framework*—was released in 2004.<sup>2</sup> This framework was created to be a benchmarking tool for an organization to assess currently adopted risk management solutions and draw a road map toward full ERM implementation.

The COSO framework was tested with certain selected companies, and its publication was accompanied by a set of application techniques. Nonetheless, there is still very little practical knowledge about how a comprehensive ERM infrastructure may be built and how it will function. Moreover, any literature on the corporate governance implications of ERM is still very limited in scope. The Conference Board Working Group on Enterprise Risk Management (working group) was instituted to fill this knowledge gap and develop a consensus on emerging practices.

This report, which represents the consensus reached by working group participants, discusses the following topics:

- What ERM is and how it differs from traditional risk management solutions.
- How legislatures, regulatory agencies, and the judiciary have been laying a legal foundation for ERM.
- The role of corporate boards, senior executives, functional managers, and business unit risk owners in the ERM infrastructure.
- What elements constitute a comprehensive ERM program.
- How corporate disclosure to stakeholders may be enhanced by ERM.

<sup>1</sup> See p. 30 for a discussion of the most recent studies.

<sup>2</sup> Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framework*, September 2004. Other ERM frameworks include the *Australian/New Zealand Standard for Risk Management 4360* (1999), the model embedded in the *King Report on Corporate Governance for South Africa* (2002), British business standard *BS 6079-3 - Project Management: Guide to the Management of Business: Related Project Risk* (2000), and *ISO/IEC Guide 73 - Risk Management: Vocabulary - Guidelines for Use in Standards* (2005).

This report is a complement to *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, a 2006 report that illustrates findings from survey-based research on how board members perceive their risk oversight role.<sup>3</sup>

Through these and other research projects on risk governance, The Conference Board Governance Center continues to address the multi-faceted issue of stock market

short-termism according to the recommendations made by delegates to the Corporate/Investor Summit held in London in July 2005. In the view of delegates to that summit, “Widespread adoption of an Enterprise Risk Management framework should be encouraged as an effective process to assess and respond to strategic and operating risk, not only to bring clarity to the long-term strategic direction a business should take, but also to clearly communicate such long-term strategy to the market.”<sup>4</sup>

---

<sup>3</sup> Carolyn Kay Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman, *The Role of the U.S. Corporate Board in Enterprise Risk Management*, The Conference Board, Research Report, R-1390-06-RR, 2006.

---

<sup>4</sup> Matteo Tonello, *Revisiting Stock Market Short-Termism*, The Conference Board, Research Report, R-1386-06-RR, 2006, p. 43.

# Key Findings

This report is the result of inquiries conducted by The Conference Board Research Working Group on Enterprise Risk Management (working group), which was instituted by The Conference Board Governance Center in September 2005 and completed its research in January 2006. Members included corporate executives (general counsel, compliance officers, risk officers, and governance professionals), consultants, and academics. Research conducted by the working group focused on emerging corporate governance standards in ERM.

## General Trends

- ERM departs from the fragmented and compartmentalized risk management solutions already in place at many companies. Its **distinctive features** include the following:
  - It is a tool to elevate risk discussions to a strategic level.
  - It is a top-down initiative, fully supported by the corporate board.
  - It offers a holistic view of the enterprise designed to capture a variety of risks throughout the firm.
- There are two facets of any risk management activity: a preventive, control-based aspect and a forward-looking and entrepreneurial aspect. Traditional risk management solutions tend to focus on negative events and often rely on diligent corporate compliance programs to control their occurrence. Given its emphasis on strategy, ERM can help the corporation find a better balance between loss-prevention, risk mitigation efforts and risk-taking, entrepreneurial endeavors.
- ERM may be used by the organization to fully uncover the value associated with intangible assets and discuss their efficient deployment in the business strategy.
- The value proposition of ERM remains under debate. Although there is a growing consensus on the strategic value of elevating risk discussions to the corporate board level, many question the cost effectiveness of establishing a complex infrastructure to achieve such a goal.
- Despite their differences in scope and emphasis, internal control procedures developed under Section 404 of the Sarbanes-Oxley Act are, in many respects, of a similar nature to those used for ERM. Although internal control processes manage financial risk and emphasize the prevention of accounting frauds, they also operate company-wide and are coordinated at the entity level. Therefore, because of the significance of the investment already made to enhance internal control, any ERM project should carefully evaluate in-house resources and leverage as many of them as possible.

## External Drivers

- The ERM efforts currently underway at many companies are influenced by several forces. Besides stakeholders' expectations, these efforts have been subject to a number of **major legal developments**:
  - the interpretation of recent Delaware case law on fiduciary duties;
  - New York Stock Exchange Listing Standards;
  - the SEC's endorsement of self-regulatory frameworks (i.e., COSO) to manage financial risk;
  - the new Exchange Act requirement to consider risk factor disclosure in annual and quarterly reports;
  - Federal Sentencing Guidelines reform; and
  - best practice standards being implemented in highly-regulated industries (e.g., banking and insurance).



- A recent survey conducted by the Tillinghast business of Towers Perrin indicates that companies have planned to set up an ERM infrastructure or have decided to improve their current ERM program based on comments received from such major **rating agencies** as Standard & Poor's and Moody's.

## ERM Infrastructure

- While many organizations have been engaging in some aspects of enterprise risk management, empirical research indicates that only a few have a full-fledged program infrastructure.
- The **role of the board of directors** includes:
  - determining a risk-adjusted corporate strategy and adequate metrics to track executive performance in the pursuit of such a strategy;
  - approving a risk inventory and fundamental ERM parameters (such as risk measurements, risk appetite, and tolerance levels) as part of the annual business plan;
  - reviewing designed procedures; and
  - overseeing the quality of the program implementation and execution, including significant expenditures made in relation to it.
- In determining its risk oversight structure, the board should conduct a preliminary **analysis of corporate governance practices**. Specifically, it should consider issues such as:
  - the independence, professional expertise, and time availability of board members;
  - the assignment of board oversight functions to specialized board committees; and
  - the quality of the information flow between board members and management.
- The board of directors should fully integrate its ERM oversight functions with **existing strategy-setting activities**. When assigning the ERM leadership, identifying new roles and responsibilities, and incorporating new protocols, the board should not alter the delicate balance already established by the reformed corporate governance standards of the last few years. Specifically, the board should ensure that the quality of existing disclosure procedures and compensation practices is not diminished.
- Research indicates that two-thirds of companies currently delegate risk oversight responsibilities exclusively to the audit committee. But a number of alternative solutions are emerging, including delegating risk oversight functions to the governance committee or the establishment of a separate **risk committee**. When separate committees are in charge of risk oversight, they should work together to marshal ERM information for the strategy-setting activities conducted by the full board.
- The role of the **chief executive officer** includes:
  - making the business case for the ERM effort and providing visible support to it;
  - contributing to the definition of the company's risk policy, risk appetite, and tolerances;
  - setting the materiality threshold (or "escalation triggers") for risk issues to be elevated through the organizational ranks;
  - determining capital allocations to finance the ERM initiative;
  - reporting to the corporate board on the outcomes; and
  - ensuring that shareholders are adequately informed about the company's long-term, risk-adjusted business strategy.



- A growing number of companies have been assigning leadership responsibilities to a **dedicated Chief Risk Officer (CRO)**. But companies should assess the time availability of existing executive positions, evaluate skills and expertise needed, determine the need to promote visibility and authority, and weigh a number of other issues before deciding whether such a position will prove a valuable contribution to the ERM effort.
- Over time, as ERM becomes fully integrated with business operations, a number of responsibilities now borne by senior executives might be **transferable to business unit leaders** and the need for a dedicated risk officer may decline.
- The knowledge of and familiarity with the organization obtained by the **Chief Financial Officer** and **Internal Auditor** in the implementation of internal control procedures are valuable and should be acquired by the leading ERM executive.
- An **Enterprise Risk Management Executive Committee** should be seen as the arena where functional managers—who have a direct working relationship with business unit managers—may voice at the executive level any concern expressed by lower organizational levels.
- Executive officers should frame the ERM infrastructure—setting the tone for the program and assigning risk ownership—**without depriving line and business unit managers of their day-to-day decisions** on the response to business uncertainties.
- The role of **business unit managers** includes:
  - responsibility for the implementation of the program within their units;
  - accountability for capital expenditures made in relation to the program execution within their units; and
  - responsibility for bringing to the attention of executives and the board risk events representing strategic opportunities.
- It is a corporate governance responsibility of board members and senior executives to understand the **economies of scope** achievable at the business-unit level through risk management integration. More specifically, they should ensure that related lines of business sharing the same risk ownership will also be sharing resources and creating opportunities for one another, while eliminating conflict-of-interest situations.
- Since proper training is essential to integrate risk management and effect the required cultural change across the organization, the quality of an **educational platform on risk management** for business unit leaders and employees should be fully discussed at the board level and should be a priority of the ERM Executive Committee.
- Since an effective monitoring function is essential to the success of ERM, in designing the program senior management should pay extra attention to the establishment of **coherent reporting lines**.

## Steps for Successful ERM Implementation

Through a number of case studies, the working group identified the following stages in the development and execution of an ERM program:

- 1 **Appreciate the importance of ERM** Board members need to become knowledgeable about ERM and appreciate its strategic value. For this purpose, they need to be provided with adequate informational materials and, if necessary, they should retain advice from independent external experts.
- 2 **Assess gaps and vulnerabilities in existing risk management solutions** The corporate board should be persuaded by the business case for implementing ERM, which should rest on a detailed analysis of the limitations inherent in current risk management solutions.
- 3 **Set underlying mission and program objectives** The ERM business case should be formulated as a concise and effective mission statement, articulated in the main program objectives, and tied to the firm's strategic goals.
- 4 **Establish the ERM infrastructure and assign leadership** As part of this step, board members and senior executives should discuss corporate risk governance policies, draft (or revise) board committee charters to incorporate ERM functions, and assign program leadership at the executive level.
- 5 **Compile a risk inventory** Risks facing the business should be identified, categorized, and prioritized. Since the accuracy of the risk portfolio is a precondition to the success of the whole program, the board should ensure that the process for inventorying risk is transparent and thorough.
- 6 **Select assessment techniques and define risk appetite and tolerance** The selection of appropriate risk measurements should be based on the nature of each risk in the portfolio, the amount and depth of data required to apply the measure being considered, and the organizational capacity of the business unit in charge of responding to the risk event.
- 7 **Determine risk response strategies** Risk owners are accountable for the response to events assigned to their area of responsibility. Nonetheless, because of the comprehensive and cohesive nature of the ERM program, their response should no longer be disjointed from other divisions of the firm and should be taken according to a set of response criteria and guidelines (the "response strategy") predetermined as part of the designed procedures. A response strategy should be developed for each risk category in the portfolio.
- 8 **Develop effective internal communication and reporting protocols** An internal flow of information is essential to the success of ERM. Therefore, in designing the program, senior management should pay extra attention to establishing coherent communication and reporting practices. Board members, for their part, should analyze the quality of internal reporting lines and be persuaded that information on risk that is material for strategic purposes will be channeled upstream and brought to their attention.
- 9 **Monitor ERM implementation and execution** In an integrated risk management environment, any activity conducted to identify, assess, and respond to risk should be monitored on an ongoing basis. Monitoring functions are embedded in the program and assigned to any organizational level so that they can be performed in the ordinary course of running a business. Large companies avail themselves of dedicated evaluation teams and sophisticated flowcharts and diagrams to ensure the enterprise-wide ramification of the monitoring function.
- 10 **Choose compensation policies and performance metrics to promote and track the pursuit of a risk-adjusted corporate strategy** The board should never let executive compensation issues influence the risk measure selection process. Although companies may decide to use qualitative and quantitative risk data as key performance indicators (KPIs) to encourage the enhancement of their business risk management program, corporate boards should ensure that KPIs are chosen only after completing the ERM process design.
- 11 **Integrate ERM with existing operational systems (i.e., IT, accounting/budgeting/planning, internal control, regulatory compliance, etc.)** Working group case studies indicate that revisiting performance metrics to tie them to a risk-adjusted strategy and fully integrating ERM with existing operational systems represent the most advanced (and least implemented) stages in an ERM program.

## Enhancing Public Disclosure on Business Risk and Long-Term Strategy

- Current SEC disclosure on risk contributes little knowledge to the investment process and is often overlooked by financial analysts. By enhancing corporate communications on risk to the public, a company that is implementing ERM can ensure that the stock market factors the value of the organizational effort into the stock price.
- With respect to the oversight of business risk disclosure, the role of the corporate board should be to:
  - ensure a high-level discussion on **how to convey** to securities analysts and investors the value inherent in the company's ERM effort;
  - verify that ERM is **fully integrated** with existing corporate disclosure procedures;
  - be satisfied with the **transparency** of the disclosure process;
  - verify the adequacy of authorization and other **verification protocols**; and
  - discuss the promotion of a **voluntary trial program** (involving a select group of financial analysts and institutional investors) for the dissemination of enhanced disclosure on long-term, risk-adjusted strategic goals.

# A Top-Down, Strategic, and Holistic Approach To Risk Management

Corporate organizations have historically put in place some form of risk management processes to protect their tangible assets and insure their business against uncertainties. In the past, these solutions were often fragmented, left to the sensitivity of functional managers or the initiative of single business unit risk owners, and unrelated to a comprehensive vision of the enterprise's long-term goals.<sup>5</sup> In addition, because of the limited budgetary resources traditionally devoted to risk management programs (and often available only to internal audit and insurance departments), those efforts did not go beyond protecting the company from the most significant, insurable risks.

ERM departs from this traditional approach by conceiving risk management as a top-down, strategic effort that requires the widest possible view of risk.

## Elevating Risk Discussions To a Strategic Level

While companies are adopting a variety of approaches to manage risk and new practices are publicized regularly, it has become clear that ERM should not be reduced to yet another loss-prevention compliance exercise.

For members of The Conference Board working group, this means being aware of the potential hidden in a business risk so that ERM may be used effectively as a tool to identify long-term strategic opportunities and elevate them to the attention of senior executives and the board. In this report, the potential benefit that the company may derive from undertaking a calculated risk is referred to as “**upside risk**.” On the other hand, those events assessed by the firm as negative or requiring a mitigation or avoidance response are termed “**downside risks**.” (See “Upside Risks and Downside Risks: A Rationale for a Distinction” on page 13 for more information on these definitions.)

The working group discussed two facets of any risk management activity: a preventive, control-based aspect and a forward-looking and entrepreneurial aspect. Traditional risk management solutions tend to focus on negative events and often rely on diligent corporate compliance programs to control their occurrence. The downside of this approach is that the company may, over time, develop a risk-averse culture. Given its emphasis on strategy and the coherent use of risk appetite and tolerance metrics, ERM can help the corporation find a better balance between loss-prevention, risk-mitigation efforts and risk-taking entrepreneurial endeavors.<sup>6</sup>

To survive in a constantly changing business environment, a corporation needs to think dynamically. This includes regularly reviewing its objectives to ensure they capture emerging opportunities and factor in new uncertainties. As a set of processes and behavioral protocols,

<sup>5</sup> Today, the matrix hierarchy (combining both functional and divisional articulations) is one of the most common business organization designs. In a business organization adopting a matrix hierarchy, activities pertaining to a particular managerial function (such as R&D, manufacturing, marketing, corporate planning, business development, personnel, finance, audit, legal, compliance, and risk) are organized into entity-level departments, while activities pertaining to a specific product or regarding a regional market are organized into business units or divisions. “Functional manager” (or “line manager”) is therefore an entity-level manager who heads one of the functional departments, as distinguished from a “business unit manager.” On this distinction and the economics of a matrix hierarchy, see, for example, Milton Harris and Arthur Raviv, “Organization Design,” *Management Science*, Volume 48, Issue 7, 2002, pp. 852–865.

<sup>6</sup> On the shift from a defensive to a more offensive and strategic focus, see, for example, Lisa Meulbroek, “Integrated Risk Management for the Firm: A Senior Manager’s Guide,” *Journal of Applied Corporate Finance*, Volume 14, Number 4, 2002, pp. 56–70.

ERM provides the infrastructure to tie a company's strategy-setting activities to a sound, risk-based analysis of its operating environment.

Taking calculated risks is essential to any business pursuing growth and expansion. Therefore, a company should find value in risk management processes devised to encourage opportunity-seeking behaviors with a realistic risk assessment conducted as part of business planning, budgeting, and forecasting.

### Upside Risks and Downside Risks: A Rationale for a Distinction

According to the COSO *Enterprise Risk Management – Integrated Framework*, an event is “an incident or occurrence, from sources internal or external to an entity, that affects the achievement of objectives,” whereas risk is more specifically defined as “the possibility that an event will occur and adversely affect the achievement of objectives.”\* Members of the working group concluded that any approach to ERM implementation needs to underscore the strategic potential inherent in many business events and risks. This report, therefore, uses the terms “risk” and “(risk) event” interchangeably, as they encompass both the potential loss and the strategic opportunity that should be addressed by an integrated risk management program. To refer to these two dimensions of a risk event, working group members used the terms “downside risk” and “upside risk.”

\* See Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework, Executive Summary*, September 2004, p. 4.

### A close correlation with corporate governance

Corporate governance is a set of corporate practices whereby boards of directors provide oversight of senior management as it executes business strategy. ERM oversight procedures add to those practices and ensure that they are adjusted to the company's risk tolerance and appetite. In the last few years, corporate governance standards have been tightened by regulators and self-regulatory bodies. Public companies have made significant progress in adapting to new rules and implementing best practices, and a growing number of studies are indicating a positive response from the stock market in terms of higher share prices.<sup>7</sup> Information on risk acquired through ERM and disseminated within the organization helps managers and board members execute their corporate governance responsibilities.

Working group participants debated whether ERM could be viewed as a key factor that complements corporate governance in a shareholder value-creation strategy (See “Benefits and Determinants of ERM” on page 18).

Although most agreed there is a strategic value to elevating risk discussions to the corporate board level (which is where long-term objectives are identified), a number of

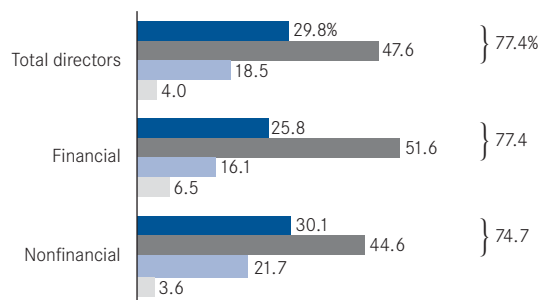
<sup>7</sup> It should be emphasized that evidence of a link between corporate governance and stock performance is still somewhat controversial, especially when the analysis is based only on a limited number of governance measures (i.e., anti-takeover defenses, self-dealing procedures, etc.). For the most recent studies supporting the correlation, see “GMI Governance and Performance Analysis,” *GovernanceMetrics International*, March 2004; Lucian Bebchuk, Alma Cohen, and Alan Ferrell, “What Matters in Corporate Governance?” 2005 Harvard Law School Discussion Paper No. 491, 2005; and Paul Gompers, Joy Ishii, and Andrew Metrick, “Corporate Governance and Equity Prices,” *Quarterly Journal of Economics*, Volume 118, Number 1, 2003, pp. 107-155.

## ERM as a Strategic Effort: What Do Corporate Directors Think?

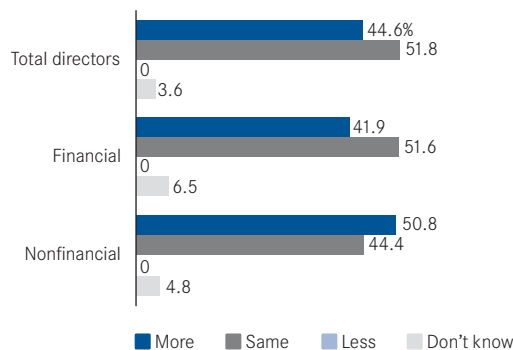
A 2006 survey of directors conducted by The Conference Board with McKinsey&Company and KPMG's Audit Committee Institute probed corporate board members' perception of ERM to verify whether its contribution to boards' strategy-setting activities is truly understood. A number of questions included in the survey tested the awareness of the correlation among aspects such as risk assessment and mitigation, strategic value creation, and compensation policies. As responses in Chart 1 indicate, directors have a high degree of appreciation for such a correlation; moreover, they are in favor of using sound risk analyses as a tool to define or revise their companies long-term strategic objectives.

Chart 1

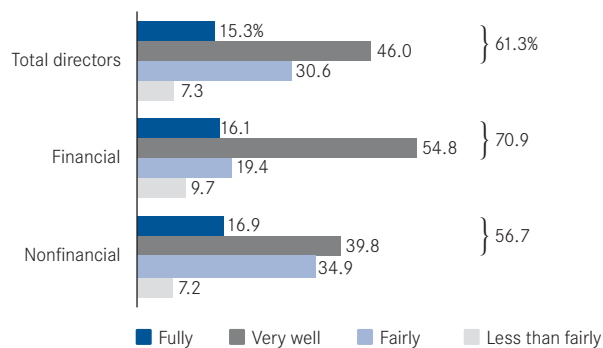
**How well does the board understand how business risks could impede the implementation of the current corporate strategy?**



**Would the board like to see more or less risk analysis pertaining to the corporate strategy?**



**How well does the board understand potential conflicts between the corporate strategy, risk occurrence, and the executive compensation policy?**



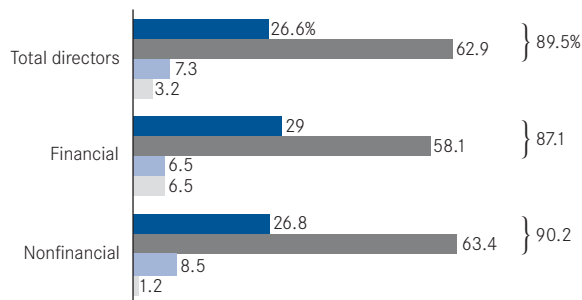
Note: Percentages may not add to 100 percent due to rounding.

Source: Carolyn Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman, *The Role of U.S. Corporate Boards in Enterprise Risk Management*, The Conference Board, Research Report, R-1390-06-RR, 2006, pp. 18–19. Data is based on a survey of 127 corporate directors in the United States.

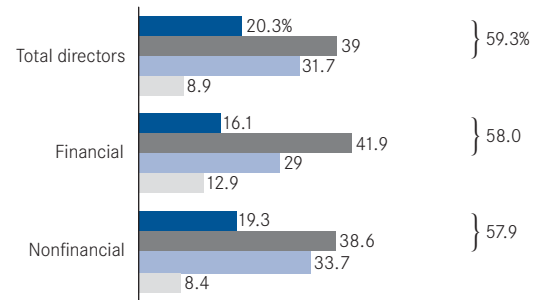
On the other hand, answers provided to other questions in the survey suggest that there is room for further improvement of oversight practices. For example, responses indicate that corporate boards are somewhat less confident about separating the potential rewards (upside) from the potential losses (downside) of risky endeavors inherent in business strategy. In fact, while few state that their board does not understand the risk implications of corporate strategy, many recognize that the board's familiarity with the risk/return tradeoff underlying such a strategy is not more than "fair" (Chart 2). Therefore, the study concludes that—because of a false sense of security—directors may not really know whether their companies are appropriately compensating themselves for the risk they are undertaking.

Chart 2

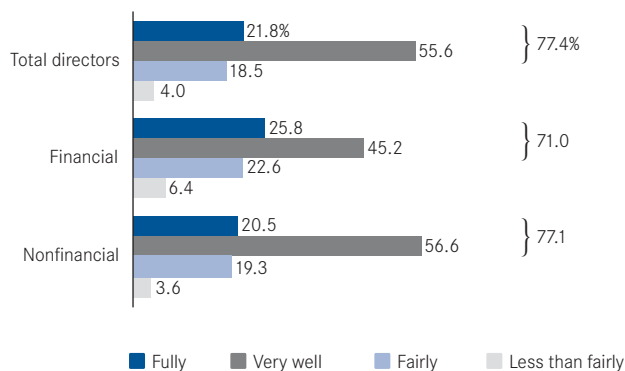
**How well does the board understand the risk implications of the current corporate strategy?**



**How well does the board understand how business segments interact in the overall company's risk portfolio?**



**How well does the board understand the risk/return tradeoffs underlying the corporate strategy?**





them questioned the cost effectiveness of a formalized framework intended to achieve such a goal. Specifically, one observed that “the experience of Sarbanes-Oxley Act Section 404 implementation suggests that any preliminary cost/benefit analysis is destined to be revised at a later stage, where expenses turn out to be far higher than the immediately quantifiable benefits resulting from the effort.” Still, for the reasons given below, the issue of ERM’s ultimate cost should not be overstated.

### Building a stable platform

As a result of the mandated effort to comply with the Sarbanes-Oxley Act, companies now have a platform on which to build their ERM infrastructure. This base consists of sets of protocols and procedures specifically designed to assess, test, and provide feedback on the effectiveness of internal controls over financial reporting. Since 1992, COSO, which originally developed the ERM framework, has been publishing benchmarks for building an internal control infrastructure.<sup>8</sup> Therefore, despite their differences in scope and emphasis, such internal control procedures are, in many respects, of a similar nature to those found in ERM. In 2004, COSO stated that its internal control framework is “encompassed within and an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk.”<sup>9</sup>

Acquired knowledge and expertise on managing financial risks offer a valuable springboard for ERM development. Because of the significance of the investment already made to enhance internal control, any ERM project should move from the evaluation of in-house resources and leverage lessons learned in complying with the Sarbanes-Oxley Act.

### Cascading the View from the Top

Working group members cited the “tone at the top” of the business structure as the second most crucial feature of an ERM framework. Although most of the surveyed executives confirmed that practically every organization somehow deals with risks on a day-to-day basis, the working group acknowledged that, in practice, a bottom-up approach to risk management remains the most common. This means that it is often left to the discretion of the single business unit to assess the relevance of a risk issue and decide if it requires an immediate mitigation response and if it should be raised to higher ranks in the chain of command or should simply be disregarded as immaterial.

With ERM, this approach is inverted and managing risk becomes a cohesive ongoing activity led by senior management and overseen by the corporate board. While the bottom-up risk management solution is a reactive, ad hoc response to negative events, a top-down ERM framework is designed to be an anticipatory procedural tool to ensure that risk is fully understood—even before its occurrence—in its negative and positive components.

In ERM, the corporate board provides the impetus for any needed organizational change, oversees the coherence of the program designed and implemented by senior management throughout the enterprise, and ensures that the corporate culture supporting ERM is aligned with the firm’s long-term strategic objectives.

To fulfill their fiduciary duties, members of the board should initiate discussions on risk and strategy, remain abreast of emerging practices in the field, and encourage senior management to adopt them. Also, directors should insist that new risk-taking ventures are supported by evidence resulting from a consistent application of robust risk assessment techniques.

Working group participants reported a number of situations where boards of directors were uninformed about risk management practices being developed by corporate executives; risk discussions would take place at the board level, but they would often be isolated and lack coordination with operational activities. Any effective approach to ERM, therefore, requires a departure from this tradition.

<sup>8</sup> COSO, *Internal Control – Integrated Framework*, 1992. This model has now been adopted by many public companies around the world.

<sup>9</sup> COSO, *Enterprise Risk Management – Integrated Framework*, 2004, Appendix C, p. 109.

Although the responsibility for the implementation of risk management processes remains with senior managers, the corporate board is the main sponsor and supporter of the ERM effort as well as, in its oversight capacity, the final recipient of the knowledge on risk that ERM brings to the organization. The whole infrastructure designed by corporate executives should facilitate such a flow of information from and to the top level.

In the current regulatory and business environment, directors should be engaged in the program and satisfied about the ultimate value it adds to their strategy-setting activities. To this end, their oversight role should extend to such fundamental components of ERM as the development of a corporate policy and a common language on risk, the compiling of a risk inventory, and reaching consensus on the company's risk profile and tolerance (see "ERM at Work" on page 43).

## Capturing Risk across the Enterprise

The Sarbanes-Oxley Act's impact on internal control is narrowly focused on managing the risk of fraud and ensuring accurate financial reporting. ERM, on the other hand, encompasses a wider array of the business risks the corporation is exposed to, including strategic and operational risks. In order to be successful, the program needs to be embedded in, and supported by, the entire firm.

The impact of certain risks on the corporation may be catastrophic. Examples include the recall of a defective product, the sudden need to close a production facility due to *force majeure* events, the underperformance of a business unit, an unexpected regulatory change, or the filing of an employee class action. In addition, the implication of such events to the firm's reputation represents a risk of its own that is often the least assessable and insurable of all. Risk-related losses can also lead to unfortunate headlines (see Table 1).

Because of its portfolio view of business risk, a comprehensive ERM framework has **crossfunctional ramifications** across the enterprise, and is integral to running the business.<sup>10</sup> As opposed to dealing in isolation with incidents, ERM fosters consistency in a company's response to the downside of risk and ensures that its long-term strategic potential is captured, raised to higher corporate ranks, and, if material, considered at the board level. The board's input on the development of the program and the use of a widely-recognized terminology favor a coherent approach to risk management throughout the firm.

<sup>10</sup> On the holistic aspects of ERM, see, for example, Jerry A. Miccolis and Samir Shah, *Enterprise Risk Management: An Analytic Approach*, Tillinghast-Towers Perrin, 2000.

Table 1

### Recent Examples of Risk-Related Losses

Type of Loss	Company	Details
Market	Ford	\$952 million write-down on stockpile of palladium in 2002
Credit	JP Morgan Chase	\$1.4 billion loss in telecom loans in 2002
Operational	The Bank of New York	\$140 million loss post-9/11—backup systems on the same power grid
Business volume	United Airlines	Bankruptcy filing due, in part, to declines in air traffic volume in 2002
	Schering-Plough	Clarinx sales suffer due to delayed launch and increased market share of geriatric drugs

Source: McKinsey&Company, 2006.

## Benefits and Determinants of ERM

Despite the lack of empirical evidence proving ERM's worth, academic studies and survey-based research have elaborated on the benefits and determinants of an integrated, top-down approach to managing business risk.<sup>\*</sup> Particular emphasis has been put on **internal determinants** (i.e., those benefits that can be assessed in the form of increased shareholder value). According to this literature, ERM:

- Reduces the inefficiencies inherent in the traditional, segmented approach to risk management and promotes cost reductions through the development of synergies among business units and departments.
- Minimizes costly risk exposures by allowing the company to identify interdependencies among risks that would remain unnoticed under the traditional risk management model.
- Provides—through its emphasis on overall risk appetite—a more objective basis for resource allocation, therefore improving capital efficiency and return on equity.
- Stabilizes earnings and reduces stock price volatility. Empirical evidence, especially in the insurance industry, supports the use of hedging techniques to reduce unanticipated earnings fluctuations; further studies insist on the need to coordinate hedging activities among traditional silos in order to optimize their benefits.<sup>\*\*</sup>
- Offers the tools to make more profitable, risk-adjusted investment decisions.
- Improves transparency to stakeholders, thereby reducing regulatory scrutiny, litigation expenses, costs of access to equity capital, and the rate of return on incurred debt.

It is expected that business organizations suffering higher stock-price volatility, resource allocation inefficiencies, reputational issues related to financial opacity, or excessive costs of capital will value an integrated approach to risk management and decide to undertake the effort of fully implementing ERM. Likewise, firms pursuing an

expansive strategy should perceive the importance of a program that will help them assess and choose the best business opportunity.<sup>\*\*\*</sup>

For a discussion of certain **external factors** (such as pressures from stakeholders and regulatory developments) that are driving firms to integrate their risk management activities, see “The Legal Foundation of Enterprise Risk Management” on page 21. Additional external influences examined by researchers include industry consolidation processes and the technological progress enabling better risk identification and assessment. Since the strengthening of corporate governance regulation in the United States in 2002, external factors have provided the primary impetus for implementing ERM. On the other hand, the importance of internal drivers grows as ERM becomes more widespread and its value is more fully understood (Table 2 and Chart 3).

\* For an overview of the benefits summarized in this box, see André P. Liebenberg and Robert E. Hoyt, “The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officers,” *Risk Management and Insurance Review*, Volume 6, Issue 1, 2003, pp. 37–52. Among other academic sources, see, for example, Tim S. Campbell and William Kracaw, “Corporate Risk Management and the Incentive Effects of Debt,” *Journal of Finance*, Volume 45, Number 5, 1990, pp. 1673–1686; Christine M. Cumming and Beverly J. Hirtle, “The Challenges of Risk Management in Diversified Financial Companies,” *FRBNY Economic Policy Review*, March 2001, pp. 1–17; Michael Haubenstock, “Organizing a Financial Institution to Deliver Enterprise-Wide Risk Management,” *Journal of Lending and Credit Risk Management*, Volume 81 (1999); Lisa Meulbroeck, “A Senior Manager’s Guide: Integrated Risk Management,” *Journal of Applied Corporate Finance*, Volume 14, Issue 4, 2002; Kent D. Miller, “A Framework for Integrated Risk Management in International Business,” *Journal of International Business Studies*, Volume 23, Issue 2, 1992, pp. 311–331; and Clifford W. Smith and Rene M. Stulz, “The Determinants of Firms’ Hedging Policies,” *Journal of Financial and Quantitative Analysis*, Volume 20, Number 4, 1985, pp. 391–405. For the most recent survey-based literature, see *CFO Research Services, Strategic Risk Management: New Disciplines, New Opportunities*, CFO Publishing Corp., 2002, available at [www.aon.com](http://www.aon.com); and Tillinghast-Towers Perrin, *Enterprise Risk Management in the Insurance Industry – 2002 Benchmarking Survey Report*, available at [www.tillinghast.com](http://www.tillinghast.com).

\*\* Lee L. Colquitt and Robert E. Hoyt, “Determinants of Corporate Hedging Behavior: Evidence from the Life Insurance Industry,” *Journal of Risk and Insurance*, Volume 84, Number 4, 1997, pp. 649–676.

\*\*\* For two case studies on the use of ERM in an acquisition (The BOC Group) and to evaluate investment opportunities (Norske Skog), see Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, The Conference Board Research Report, R-1363-05-RR, 2005, p. 18 and p. 34, respectively.

Table 2

**Companies with advanced ERM experience greater returns...**

	<i>Advanced ERM companies</i>		<i>All other companies</i>	
	<i>Rank</i>	<i>Percent</i>	<i>Rank</i>	<i>Percent</i>
Better-informed decisions	1	86%	1	58%
Greater management consensus**	2	83	5	36
Increased management accountability***	3	79	7	34
Smoother governance practices***	3	79	3	39
Ability to meet strategic goals***	5	76	5	36
Better communication to board <sup>+</sup>	6	69	2	52
Reduced earnings volatility**	7	62	4	37
Increased profitability**	8	59	8	33
Use risk as competitive tool**	9	46	9	22
Accurate risk-adjusted pricing*	10	41	10	21

\*\*\* 99.9% likelihood of significant difference between advanced ERM and all other companies

\*\* 99% likelihood of significant difference between advanced ERM and all other companies

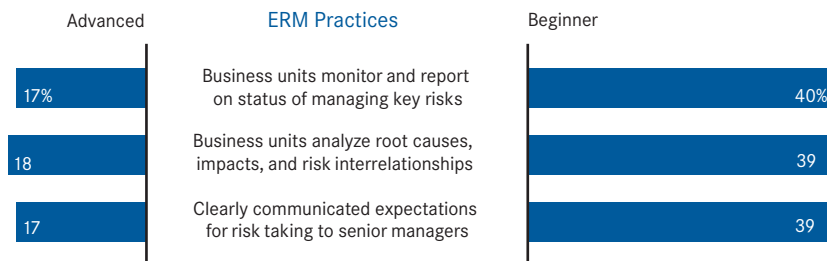
\* 95% likelihood of significant difference between advanced ERM and all other companies

<sup>+</sup> 90% likelihood of significant difference between advanced ERM and all other companies

Chart 3

**...and are less likely to view ERM as a routine procedure**

Percent responding "ERM is just another layer of bureaucracy"



Source: Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, The Conference Board Research Report, R-1363-05-R, 2005, p. 32. Data is based on a survey of management executives from 271 companies based in North America and Europe.

As a result of this complex but coordinated effort, the whole organization's sensitivity to uncertainties should be enhanced. With time, each employee should acquire the necessary sensitivity and discipline to contribute to the enterprise-wide risk management program, attributes that are required for a new corporate culture geared toward the ongoing assessment and management of uncertainties. Specifically, in a fully-fledged ERM environment, each employee should feel free to express risk-related concerns without fear of retribution.

In addition to capturing a large variety of risks, a corporation may also use ERM to fully uncover the value of its intangible assets and discuss their efficient deployment in the business strategy. Asset items (e.g., intellectual property, innovative marketing practices, and research and development (R&D)) carry tremendous potential, which should be embraced by the firm. Thanks to its enterprise-wide scope, ERM may be the tool to reveal intangibles that would otherwise remain hidden, ensuring that they are inventoried and considered when the corporate strategy is set or reviewed.

## Unlocking the Hidden Value of Intangible Assets<sup>11</sup>

Historically, manufacturing companies have derived most of their firms' value from tangible assets like plant and equipment. In a modern, knowledge-based economy, however, the sources for corporate profits are more likely to be found in a variety of intangible assets, including the

output of employees' creativity (for which the company may obtain legal protection through copyrights, patents, and trademarks), innovative production mechanisms or marketing processes, know-how, workforce expertise and professional development, quality controls, and customer satisfaction.<sup>12</sup>

Increasingly, organizations must be able to rely on an enterprise-wide process that:

- Maintains an asset inventory where intangibles are classified by, among other criteria, their nature, their location, their immediate availability, and the risk exposure borne by them.
- Quantifies their intrinsic value, determines their propensity to be strategically deployed, assesses their impact on risk appetite, and evaluates their actual contribution to the long-term growth of the business.
- Develops a set of extrafinancial measures of performance appropriate to assess whether intangible assets are being adequately deployed. (See "Enhancing Public Disclosure through ERM" on page 83.)
- Clearly communicates such information to the market.

If adequately implemented, an enterprise-wide process of this sort ensures that business potentials are unlocked and the company is set to meet its long-term objectives.

<sup>11</sup> Much of the material in this section originally appeared in Tonello, *Revisiting Stock Market Short-Termism*, p. 28.

<sup>12</sup> On the nature and qualities of intangibles, see Baruch Lev, *Intangibles: Management, Measurement, and Reporting*, Brookings Institution Press, 2001. In Lev's work, intangible assets are classified in the three broad categories of discoveries, organizational practices, and human resources. For recent data on the impact of intangibles assets on certain countries' economies, see *Data For Intangibles in Selected OECD Countries*, OECD and Statistics Netherlands, 2005, available at [www.oecd.org](http://www.oecd.org).

# The Legal Foundation of Enterprise Risk Management\*

The financial disruptions of the last few years revealed the inability of many business organizations to effectively assess and manage their risks. Stemming from those corporate debacles and driven by the evolving expectations of stakeholders, a number of recent legal, regulatory, and best practice developments are redefining director duties and strengthening executive accountability in the area of risk management.

## The Expanding Scope of Fiduciary Duties under Delaware Corporate Law

Under state law, directors owe fiduciary responsibilities to the corporation and its shareholders. Traditionally, the corporate law of Delaware (where a vast majority of Fortune 500 businesses are incorporated) has required directors to act with loyalty to the corporation and exercise care in the performance of their duties.

The “business judgment rule” is often cited as the main standard by which Delaware courts review director conduct. By establishing a presumption that directors act loyally and diligently, the business judgment rule has been the crucial legal foundation of risk undertaking. Because of the protection they receive from the rule, directors, in turn, are encouraged to embrace entrepreneurial risks and pursue the strategic opportunities originated by those risks. Generally speaking, under the rule, board members are not liable for a bad business decision unless their conduct is in violation of fiduciary duties.

The August 2005 *Disney* decision by the Delaware Court of Chancery, later upheld by the Delaware Supreme Court, provides some important insights into the scope of fiduciary duties. While upholding the validity of the business judgment rule, Chancellor William Chandler underscored the importance of good faith in the performance of corporate duties and stated that directors and officers are expected to fully understand current best practices as well as ensure that business decisions are made in light of widely-recognized corporate governance standards.<sup>13</sup>

The immediate implication of the *Disney* decision in the area of enterprise risk is that risk management best practices, even though they are just emerging, do matter and could be a standard of review of fiduciary liability. To be sure, the judiciary interpretation of the *Disney* case should be read in connection with the principle, established in the earlier *Caremark* case, that a board has an obligation to “exercise a good faith judgment that the corporation’s information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations.”<sup>14</sup>

\* An earlier version of this section appeared in Brancato et al., *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, Appendix II, pp. 33–37.

<sup>13</sup> *In re The Walt Disney Co. Derivative Litig.*, Cons. C.A. No. 15452, 2005 Del. Ch. LEXIS 113 (Del Ch., Aug. 9, 2005). Also see Cons. C.A. No. 15452 (Del. Supr., June 8, 2006). For a statutory requirement to act in good faith, see Section 102(b)(7) of the Delaware General Corporation Law, which permits a corporation to include in its articles of incorporation a provision eliminating or limiting a director’s personal liability for monetary damages for breach of fiduciary duty so long as there are no “acts or omissions not in good faith.” The standard for determining whether one has acted in good faith may depend on the director’s degree of personal knowledge and expertise; for further information, see Carolyn K. Brancato and Alan Rudnick, *The Evolving Relationship Between Compensation Committees and Consultants*, The Conference Board, Research Report, R-1382-06-RR, 2006, citing the recent *In re Emerging Communications, Inc. Shareholder Litigation* decision by the Delaware Court of Chancery (2004 Del. Ch. LEXIS 70), where a director was found personally liable for breach of good faith because—due to his financial expertise—he was in a “unique position to know” that a merger price was not fair.

<sup>14</sup> *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. Sept. 25, 1996).



In the post-*Disney* state law environment, therefore, directors should consider overseeing the development of risk management best practices and remain apprised of the state of the art in that area. Accordingly, executives and senior managers should be held accountable by their directors for the implementation of risk management processes and for ensuring that there is an adequate flow of information to the board and shareholders on how the company is prepared to respond to risk factors affecting business operations.

## Federal and Regulatory Requirements

While it did not specifically mandate on risk management, the Sarbanes-Oxley Act of 2002 was the congressional response to the poor quality of corporate disclosure revealed by the corporate scandals and a wave of financial restatements. Among other things, the new statute requires chief executives to establish (and report on the effectiveness of) internal control and disclosure procedures.<sup>15</sup> According to the subsequent regulation enacted by the Securities and Exchange Commission (SEC), such a set of procedures should be designed according to a “suitable, recognized control framework.” The SEC specifically recommends the use of COSO’s 1992 *Internal Control–Integrated Framework*.<sup>16</sup>

Implicitly, the SEC endorsed the COSO approach to managing financial fraud risks, where internal control is “a process, effected by an entity’s board of directors, management, and other personnel” and based on the mapping and assessment of the risks a company is exposed to.<sup>17</sup> While it states that Sarbanes-Oxley requirements are limited to the area of internal control and the risk of fraud, the SEC clearly encourages management to pay attention to a broader spectrum of risks and to manage them in an enterprise-wide context. (See “An Implicit Endorsement of Enterprise Risk Management” on page 23 for more evidence supporting this interpretation.)

In addition, to “enhance the content of Exchange Act reports and their value in informing investors and the market,”<sup>18</sup> the SEC has extended to periodic filings on Form 10-K and Form 10-Q the same requirement to consider risk factor disclosure that had long been applicable under Regulation S-K to securities offering prospectuses.<sup>19</sup> The formulation of the requirement is vague and does not explicitly suggest that the company should disclose the knowledge of risk it acquired through its risk management processes. Nonetheless, discussion of such factors in annual and quarterly reports should highlight major risk issues for the attention of investors and financial analysts; ultimately, the market demand for periodic updates on risk may increase the pressure on the company to establish a comprehensive ERM infrastructure.

<sup>15</sup> See Section 404 of the Sarbanes-Oxley Act for statutory requirements on the management’s report on internal control. Also see SEC Release No. 33-8392 (September 22, 2005). In addition, under Section 302, CEOs and CFOs are required to sign an annual certification on the establishment of internal control and disclosure procedures. For a commentary on the Sarbanes-Oxley Act and SEC rules, see John T. Bostelman, *The Sarbanes-Oxley Deskbook*, Practising Law Institute, 2006.

<sup>16</sup> SEC Release Nos. 33-8238; 34-47986 (“Management’s Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports”), June 5, 2003, at text accompanying note 67.

<sup>17</sup> See COSO, *Internal Control–Integrated Framework*, 1992. In 1995, the AICPA incorporated the definition of internal control set forth in the COSO *Report in Statement on Auditing Standards* No. 78 (codified as AU §319 in the Codification of Statements on Auditing Standards).

<sup>18</sup> SEC Release No. 33-8591; 34-52056 (“Securities Offering Reform”), July 19, 2005.

<sup>19</sup> See Item 1A of Securities Exchange Act Forms 10-K and 10-Q, effective December 1, 2005. For the requirement to disclose risk factors already applicable to Securities Act registration statements and prospectuses, see Item 503(c) of Regulation S-K.



## An Implicit Endorsement of Enterprise Risk Management

The following is an excerpt from the SEC Release on Management's Report on Internal Control issued on June 5, 2003. Even though the release reaffirms the principle that any regulatory action is bound by the scope of the Sarbanes-Oxley Act, the following passage is compelling in how it reveals the Commission's view of internal control as a procedural component of enterprise risk management:

A few of the commenters urged us to adopt a considerably broader definition of internal control that would focus not only on internal control over financial reporting, but also on internal control objectives associated with enterprise risk management and corporate governance. While we agree that these are important objectives, the definition that we are adopting *retains a focus on financial reporting....* We are not adopting a more expansive definition of internal control for a variety of reasons. Most important, we believe that [the Sarbanes-Oxley Act] focuses on the element of internal control that relates to financial reporting. In addition, many commenters indicated that even the more limited definition related to financial reporting that we proposed *will impose substantial reporting and cost burdens on companies*. Finally, independent accountants traditionally have not been responsible for reviewing and testing, or attesting to an assessment by management of, internal controls that are outside the boundary of financial reporting.\*

Both the SEC and, for the banking sector, the Federal Reserve have been vocal about the need to incorporate internal control and compliance exercises into an integrated approach to managing business risk:

### Cynthia Glassman, SEC Commissioner:

"While the purpose of Section 404 is laudable—to help make sure that company financial statements are reliable and materially accurate—there has been widespread criticism of the burdens and costs of implementation. It appears that what was intended as a top-down, risk-based management exercise has become a bottom-up, non-risk-based exercise with an apparent focus on controls for controls' sake."\*\*

\* SEC Release Nos. 33-8238; 34-47986 ("Management's Reports on Internal Control Over Financial Reporting"), June 5, 2003, text accompanying note 49. Emphasis added.

\*\* Remarks at "Beyond the Myth of Anglo-American Corporate Governance," Institute of Chartered Accountants in England & Wales, Washington, D.C., December 6, 2005.

### Mark W. Olson, Governor, The Federal Reserve Board:

"A consolidated, or 'enterprise-wide,' approach to compliance risk management has become 'mission critical' for large, complex banking organizations.... Because compliance failures have touched many businesses, including banking, securities, and insurance firms, it has become clear that companies operating in more than one type of business must have a compliance strategy that is both globally consistent and locally effective. Increasingly, large, complex organizations are taking an enterprise-wide compliance-risk management approach to augment and better coordinate what had been fragmented and duplicative compliance activities. Such an approach puts local compliance activities within individual business lines into an integrated, global program, makes possible an understanding of compliance requirements and performance across an organization, and promotes consistency in responsibility, expectations, documentation, assessment, and reporting. I have been told that this more-integrated approach to compliance risk management by industry is already having a positive effect on risk identification and mitigation."\*\*\*

\*\*\* Remarks to the Financial Services Roundtable and the Morin Center for Banking and Financial Services, Washington, D.C., May 16, 2006.

## Securities Exchange Listing Standards

The New York Stock Exchange (NYSE) Listed Company Manual assigns to the company's audit committee the duty and responsibility to "discuss policies with respect to risk assessment and risk management."<sup>20</sup> Under the rule, such a responsibility should be explicitly stated in the audit committee charter.

The audit committee's role is further clarified in the commentary accompanying the set of regulatory requirements. In the commentary, the NYSE staff acknowledges that it is the job of the CEO and other senior executives to manage risk, and that the audit committee should limit its involvement to a general discussion of guidelines and policies governing the whole process. How the written interpretation reveals the nature of the risk covered by the rule is more specific than enterprise risk is even more important. In fact, the concept of "risk assessment and risk management" is explained as "the steps management has taken to monitor and control ... the listed company's major *financial risk* exposure."<sup>21</sup>

In addition, the need to address risk factors through a set of predesigned procedures emerges from the section of the NYSE *Listed Company Manual* imposing the adoption and disclosure of a code of business conduct and ethics, which "can focus the board and management on areas of ethical risk, provide guidance to personnel to help them recognize and deal with ethical issues, [and] *provide mechanisms* to report unethical conduct."<sup>22</sup>

Risk management functions are not explicitly covered by the NASD Rules.

<sup>20</sup> Section 303A.07(c)(iii)(D) of the NYSE *Listed Company Manual*, available at [www.nyse.com](http://www.nyse.com).

<sup>21</sup> See Commentary to Section 303A.07(c)(iii)(D) of the NYSE *Listed Company Manual*. Also see John T. Bostelman, Sullivan and Cromwell, "Legal Update on Risk Management Issues," Presentation to The Conference Board Working Group on Enterprise Risk Management, New York City, September 15, 2005. Emphasis added.

<sup>22</sup> See Commentary to Section 303A.10 ("Code of Business Conduct and Ethics") of the NYSE *Listed Company Manual*. Emphasis added.

## Federal Sentencing Guidelines

In response to a mandate included by Congress in the Sarbanes-Oxley Act, the U.S. Sentencing Commission has strengthened the section of its guidelines on crimes by business organizations. Ultimately, the purpose of the guidelines is to reduce any disparity in sentencing and ensure, to the greatest possible degree, certainty of criminal punishment. To do so, the Commission devised a point-based system where a numerical value is attributed to an unlawful conduct according to its degree of severity and the criminal history of the individual. The nationwide implementation of the system started in January 1989.<sup>23</sup>

Effective November 1, 2004, the new Federal Organizational Sentencing Guidelines provided for offsetting points and a more lenient treatment of executive malfeasance if the organization had established a well-functioning and qualifying compliance program. Although no particular compliance program is described, it must be reasonably designed to promote "*an organizational culture* that encourages ethical conduct and a commitment to compliance with the law."<sup>24</sup> Specifically, under the guidelines, directors and officers would benefit from criminal fine reductions if the corporation can demonstrate, that:

- It has identified areas of potential risks for criminal violations.
- It has trained senior officials and employees in the pertinent legal standards and obligations.
- It has provided "sufficient authority and resources" to compliance officers to discharge their duties, including monitoring the compliance program and reporting periodically to the board of directors on its effectiveness.
- Its directors and officers have, in fact, assumed responsibility for the oversight and management of the compliance program.

<sup>23</sup> For an overview of the United States Sentencing Commission and the Federal Sentencing Guidelines, see [www.ussc.gov/general/USSCoverview\\_2005.pdf](http://www.ussc.gov/general/USSCoverview_2005.pdf).

<sup>24</sup> See Chapter Eight ("Sentencing of Organizations"), 2004 *Federal Sentencing Guidelines Manual*, available at [www.ussc.gov/2004guid/tabconchapt8.htm](http://www.ussc.gov/2004guid/tabconchapt8.htm). Emphasis added.

- The program is articulated in a set of procedures protecting whistleblowers from retaliatory actions.
- The program is regularly revised and appropriately modified to address new risks to which the corporation becomes exposed.

It should be noted that the U.S. Supreme Court ruled in a recent decision that the mandatory nature of the guidelines is unconstitutional. In particular, the requirement that judges should calculate fines by taking into account information (such as the severity of the crime) that may not have been among the facts persuading the jury to convict a defendant was deemed in violation of the Sixth Amendment right to trial by jury. Nonetheless, the guidelines remain valid as advisory principles, and most commentators agree that the Supreme Court ruling should have no immediate effect on the sentencing mitigation compliance program that the guidelines encourage.<sup>25</sup>

## Risk-Based Capital Adequacy Frameworks in Regulated Industries (Banking and Insurance)

Banks and insurance companies have a central role in the financial markets and manage the allocation of large resources. Their business failures may have tremendous implications on the global economy. Since they are a source of systemic risk, banking and insurance activities are subject to heavy regulatory regimes. Primarily, such regimes are intended to prevent unnecessary risk exposure and to ensure that, when a risk materializes, it is adequately managed so as to avoid ripple effects on the worldwide financial system.

The New Capital Adequacy Framework for bank capital regulation, also known as Basel 2, was designed to

improve operational risk management practices adopted by financial institutions, especially in the area of credit risk.<sup>26</sup> In fact, the main premise for the work of the Basel Committee on Banking Supervision is that banks are subject to a number of operating risks resulting from ineffective or failed internal processes.

Basel 2 provides a platform for a much needed convergence of credit risk management practices in financial institutions.<sup>27</sup> Risk management is also the key differentiation from the approach used in the preexisting 1988 Basel Capital Accord, as bank capital adequacy is now assessed through a wider range of risk-sensitive standards.

Basel 2 was formally endorsed in June 2004 by central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries, including the United States. But, because of its nature as an international agreement, its implementation and enforcement depend on its adoption by way of formal legislation. The European Union has done so through the so-called Capital Requirement Directive, which calls for full implementation by the beginning of 2008.<sup>28</sup> In the United States, regulation based on Basel 2 is being developed by the SEC and Department of Treasury agencies (the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision). According to the announced timetable, Basel 2 would become the capital adequacy standard in 2009, but only

<sup>25</sup> John T. Bostelman discussed this during his "Legal Update on Risk Management Issues" presentation to the working group. For an overview, see Carolyn K. Brancato, *Enterprise Risk Management Systems: Beyond the Balanced Scorecard*, The Conference Board, Research Report E-0009-05-RR, 2005; and Harvey L. Pitt, "Fine Print: SEC Penalty Plan Explains Price of Fraud," *Compliance Week*, January 31, 2006.

<sup>26</sup> Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, June 2004. For further information and updates, visit the official website at [www.bis.org/publ/bcbsca.htm](http://www.bis.org/publ/bcbsca.htm).

<sup>27</sup> For a few examples of pragmatic applications of the Basel 2 operational risk management framework, see Benedikt Wahler, "Process-Managing Operational Risk. Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II Framework," Johns Hopkins University Working Paper, January 2005.

<sup>28</sup> European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council recasting Council Directive 93/6/EEC of March 15, 1993, on the capital adequacy of investment firms and credit institutions (COM(2004)0486 – C6-0144/2004 – 2004/0159 (COD)), available at [www.europarl.eu.int](http://www.europarl.eu.int).

for institutions with more than \$250 billion in assets or more than \$35 billion in foreign receivables.<sup>29</sup>

The insurance industry is generally further behind than the banking industry in the development of international risk-driven solvency standards. However, the European Union has tried to replicate the success of the Basel Committee initiative and has promoted the Solvency Framework Project. Solvency I became effective among EU Member States as of January 2004 and provided an initial, more fragmentary, risk-based set of capital requirements for insurance providers operating in Europe.<sup>30</sup> The intention of Solvency II, which remains under development, is to focus on an ERM approach to operational uncertainties in the sector.<sup>31</sup> If successful, the Solvency II holistic approach to risk management could foster new federal reforms in the United States, where the insurance industry is regulated by the Insurer Model Act of 1992.

## Rating Agency Scrutiny as an External Driver of ERM Implementation

The influence of external factors on the decision to adopt ERM was explored in a recent survey of more than 70 North American life insurance industry executives conducted by the Tillinghast business of Towers Perrin.<sup>32</sup>

According to the survey findings, companies are moving toward a more sophisticated stage of ERM implementation as external stakeholders, analysts, and rating agencies demand more information on the quality of risk management procedures. In particular, a majority of respondents indicate that their firms have planned to set up an ERM infrastructure or decided to improve their current ERM program based on comments received from major rating agencies such as Standard & Poor's and Moody's.

Both agencies have added a formal evaluation of corporate ERM capabilities to their overall credit rating process. As members of The Conference Board Governance Center, they presented their methodologies to the working group on ERM.<sup>33</sup>

Prodyot Samanta, director of Enterprise Risk Management at New York-based Standard & Poor's, described the application of S&P's ERM assessment framework (which is currently applied by the rating agency to the financial service, utilities, and insurance sectors).<sup>34</sup> The framework is denominated PIM for its three primary components: Policies (and Governance), Infrastructure, and Methodology. This framework is illustrated in Exhibit 1 as a three-dimensional cube. The policies-axis represents the key elements of the ERM program reviewed by the rating agency.<sup>35</sup> The infrastructure-axis contains attributes such as the robustness of a firm's risk architecture and back-office technology, including the caliber of the personnel responsible for executing the program. Finally, the methodology-axis represents the quality of valuation techniques and other assessment metrics used by the company to measure the impact and likelihood of risk events. (For specific cube elements, see "Components of PIM.")

<sup>29</sup> In addition, to prevent a sudden drop in capital levels, they will not be allowed to decline more than 5 percent per year in each of 2009, 2010, and 2011. On the issues raised by the New Basel Accord in the United States, see Marc R. Saidenberg and Til Shuermann, "The New Basel Accord and Questions for Research," Federal Reserve Bank of New York, Wharton Financial Institutions Center Working Paper No. 03-14, May 2003.

<sup>30</sup> Directive 2002/13/EC of the European Parliament and of the Council of 5, March 2002, amending Council Directive 73/239/EEC as regards the solvency margin requirements for non-life insurance undertakings, *Official Journal* L 077, 20.03.2002, pp. 17-22.

<sup>31</sup> For an overview, see Martin Eling, Hato Schmeiser, and Joan T. Schmit, "The Solvency II Process: Overview and Critical Analysis," Universität St. Gallen Working Paper, December 2005.

<sup>32</sup> Jack Gibson and Hubert Muller, *Life Insurance CFO Survey #13: Enterprise Risk Management*, Towers Perrin Tillinghast, May 2006, p. 2. Respondents primarily included CFOs from large and mid-size North American life insurance companies; 52 percent had assets of \$5 billion or more and 21 percent were multinationals.

<sup>33</sup> For an earlier discussion of these methodologies, see Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, The Conference Board Research Report, R-1363-05-RR, 2005, pp. 22-25. In both cases, ERM assessments are just a component of the overall credit rating process. Neither Standard & Poor's nor Moody's issue separate ERM ratings.

<sup>34</sup> Prodyot Samanta, Standard & Poor's, "Assessing ERM Practices at Financial Institutions," Presentation to The Conference Board Working Group on Enterprise Risk Management, New York City, November 2, 2005. Also see *Enterprise Risk Management for Financial Institutions: Rating Criteria and Best Practices*, Standard & Poor's, November 2005.

<sup>35</sup> Also see "ERM at Work" on p. 43 for a case-study-based discussion of the procedural phases of the ERM program.

## Components of PIM

### *Policy and Governance*

**Risk Culture** What is the stature of the leading risk management executive (such as the CRO, if present) within the organization? Is the CRO in a position to act independently? How is he or she compensated? What are the CRO's reporting lines?

**Risk Appetite and Strategy** What criteria does the firm apply to determine its risk appetite and select tolerance parameters? Are such criteria customized to reflect the size of the institution and the industry it operates in?

**Risk Control and Monitoring** Do risk responses provided by risk owners conform to the firm's risk profile, appetite, and tolerance levels? What is the quality of risk reports (in terms of clarity, depth, and frequency)? What are the key elements of discussion with board members and senior management and what feedback is provided?

**Risk Disclosure** How accurate is the communication and disclosure on risk, both within the firm and to stakeholders? Does the firm proactively disclose more than required by the SEC?

### *Infrastructure*

**Architecture** Is the architecture adopted functional to the goals the firm intends to achieve through ERM (i.e., a risk-adjusted strategy and risk-based decision making)? Is the architecture cost efficient and transparent? What is the degree of integration between risk management and other corporate systems (IT, legal, compliance, operations, etc.)?

**Back-Office Operations** How robust is the technology used to manage business risk? Is the firm prepared to respond to system failures or other business disruptions? What is the caliber of personnel responsible for executing ERM procedures?

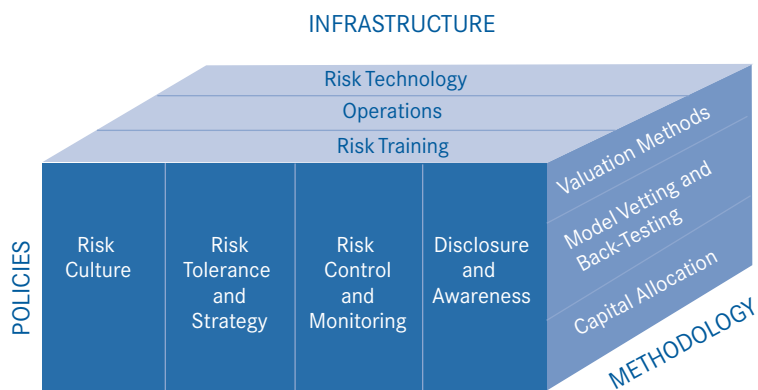
### *Methodology*

**Valuation Techniques** Did the firm choose appropriate measures (such as value at risk (VaR)) to assess the impact and likelihood of risk events? Does the company also avail itself of a set of qualitative measures, for example, to determine whether management can draw meaningful conclusions from complex quantitative metrics? How does the company track key risk indicators?

**Model Vetting and Back-Testing** Does the firm employ vetting techniques (such as stress testing and "what if" scenario analyses) to test the reliability of any adopted risk measurements?\*

Exhibit 1

### Standard & Poor's PIM Approach for Assessing ERM



Source: Prodyot Samanta, Standard & Poor's, "Assessing ERM Practices at Financial Institutions," Presentation to The Conference Board Working Group on Enterprise Risk Management (ERM), New York City, November 2, 2005.

\* For an application of the PIM Framework to assess the trading risk management (TRM) practices at 23 leading financial institutions, see *Quality of Trading Risk Management Practices Varies in Financial Institutions*, Standard & Poor's, November 28, 2005.

At another working group meeting, Hervé Geny, senior vice president and risk management specialist at Moody's Corporation, said, "A detailed ERM evaluation enriches the set of information captured through the rating process. The methodology we employ—called Risk Management Assessment (RMA)—was conceived primarily to support our credit analysts in their review of specific risk and derivatives issues (see Exhibit 2). As such, RMAs add to Moody's core analysis capabilities an accurate picture of how the issuer positions itself with respect to risk. This

picture is used to inform our final credit rating. We look at it to evaluate a firm vis-à-vis its competitors and to reflect risk profile changes the firm undergoes over time. Ultimately, we believe that a rating process that is sensitive to the quality of risk management adds value to the service we provide to fixed income investors."<sup>36</sup>

<sup>36</sup> Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on Enterprise Risk Management, New York City, January 10, 2006.

## The Four Pillars of Moody's Risk Management Assessment (RMA)

### 1 Risk Governance

- Risk governance at board and executive management level
- Risk management organization and its influence

### 2 Risk Management

- Risk control processes
- Risk appetite and limit setting
- Risk mitigation

### 3 Risk Analysis and Quantification

- Risk quantification
- Risk monitoring and reporting

### 4 Risk Infrastructure and Intelligence

- Risk infrastructure
- Risk intelligence

Note: See p. 69 and p. 79 for of Moody's gold benchmarks on risk measurement and risk intelligence, respectively.

Source: Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on ERM, New York City, January 10, 2006.



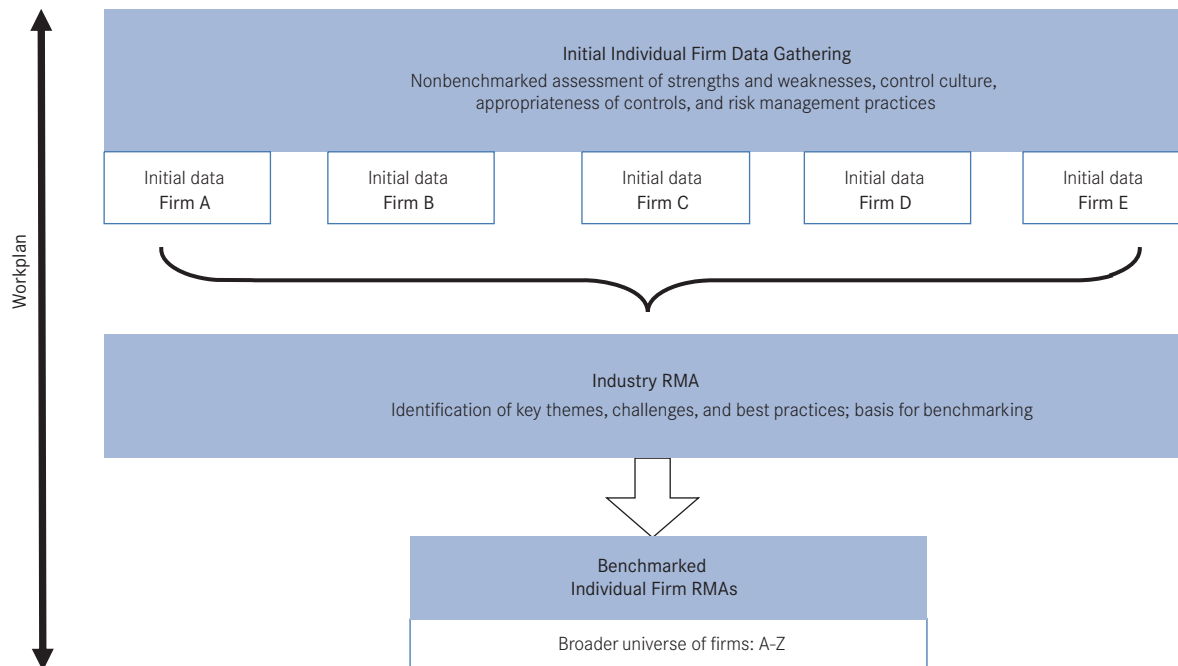
First, Moody's risk management specialists gather preliminary information on an issuer from public disclosures and any previous meeting that has taken place with management. Subsequently, they develop a structured approach (workplan) to learn more about the quality of risk management at the firm (from the board level to business lines). The goal is to understand how the risk management function is organized and how pervasive the corporate risk culture is, as well as to clarify the dynamics of risk decisions (appetite, tolerance, mitigation, and other

responses to risk) and assess the robustness of the internal risk communication and reporting framework. Finally, risk specialists hold a number of focus meetings on key areas that may directly affect the final rating, such as economic capital and risk-adjusted return, risk appetite and limits, and reporting and communication. Risk specialists also participate in Moody's rating committees, where the issuer's risk management capabilities are qualitatively weighted against other rating drivers. In the final RMA report, risk management is categorized as "strength," "neutral," and "weakness."

Exhibit 2

### Moody's RMA Approach to ERM Assessment

Analytical Process for RMA Reports



Source: Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006, p. 20.



# The ERM Infrastructure

While many organizations have engaged in some aspects of ERM, only a few have developed a full-fledged program infrastructure. Over the last few years, a number of research publications have documented the need for practical guidance to correct this situation:

- A 2002 McKinsey&Company/*Directorship* magazine survey (involving 200 directors representing over 500 boards, and released just before the Sarbanes-Oxley Act was enacted into law) found that, due to nonexistent or ineffective risk management processes, nonfinancial risks received only “anecdotal treatment” in the boardroom.<sup>37</sup>
- Management research conducted by The Conference Board in 2004 on 271 companies based in North America and Europe revealed that, despite a positive disposition toward ERM, most firms were still in the early stages of designing a comprehensive risk management infrastructure (whereas only 18 percent of surveyed corporations had a risk inventory and 15 percent had a common language for risk).<sup>38</sup> The study also found that only 16 percent of respondents had integrated advanced ERM thinking into such business practices as strategic

planning or budgeting, and even fewer (4 percent) had moved them into performance metrics or compensation policies (Table 3).

- According to PricewaterhouseCoopers’s 2004 *Global CEO Survey*, only 20 percent of the 1,400 surveyed chief executives report that they understand their accountability with respect to managing business risk.<sup>39</sup>
- A June 2006 research report from The Conference Board on corporate board practices written in collaboration with McKinsey&Company and KPMG’s Audit Committee Institute showed that, although directors are increasingly optimistic about their risk oversight abilities, few can point to the use of robust ERM techniques by their companies.<sup>40</sup>

The working group discussed a number of emerging practices regarding how ERM responsibilities are assigned within the corporate infrastructure. Discussions were based on members’ experiences, their knowledge of practices adopted by their peers, and COSO’s (or other frameworks’) application techniques.

<sup>37</sup> Robert Felton and Mark Watson, “U.S. Director Opinion Survey on Corporate Governance 2002,” Presentation of Survey Findings, McKinsey 2002. Findings are also discussed in Robert Felton and Mark Watson, “Informed Change,” *Directorship*, June 2002; and Robert Felton and David W. Anderson, “Directors and Investors Favor Further Governance Reform, not Regulation,” *Directorship*, October 2003. The study was based on 170 responses to a written questionnaire and 25 interviews.

<sup>38</sup> Gates and Hexter, *From Risk Management to Risk Strategy*, p. 27.

<sup>39</sup> *Managing Risk: An Assessment of CEO Preparedness, 7th Annual Global CEO Survey*, PricewaterhouseCoopers, 2004, p. 27.

<sup>40</sup> Brancato et al., *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*. Directors’ views of their oversight role in the context of ERM were studied through a combination of personal interviews with corporate directors, a written survey, the comparison of Fortune 100 companies’ board committee charters, and legal analysis.

## The Role of the Corporate Board and Its Committees

As mentioned earlier, ERM is a top-down initiative. The corporate board provides impetus and oversight to the program, and is ultimately responsible for ensuring that the program adds value to the business strategy-setting process. If effective, ERM can offer a risk-aware view of the company's long-term goals, which may then be adjusted to reflect the risk/reward tradeoff analysis conducted at the top level. "In an ERM environment, should the program fail to contribute to the clarity of the corporate strategy," one working group member stated, "the full board of directors would inevitably be blamed for the failure." For this reason, as Exhibit 3 on page 32 shows, the board of directors is placed at the top of the ERM infrastructure.

Risk oversight and governance functions are performed by the board of directors, alone or in collaboration with senior executives. The board's responsibilities include:

- ensuring it is apprised of evolving practices in risk management oversight;
- approving a business risk inventory, including the ranking methodology;
- approving the company's risk appetite and tolerances as part of the annual business plan;
- setting guidelines regarding the company's risk policy and ensuring that it is enforced by an effective disciplinary system;
- setting a risk-adjusted corporate strategy and ensuring adequate metrics to track executive performance;

Table 3

### Most Companies Are in the Early Stages of ERM Implementation

Basic elements of ERM identification, infrastructure, and process		Midpoint elements of ERM identification, infrastructure, and process		Advanced ERM: Integration with corporate practices	
	<i>Component is "up and running"</i>		<i>Component is "up and running"</i>		<i>Component is integrated</i>
BUs determined risk mitigation strategies	22%	Quantified key risk to best extent possible	19%	Strategic planning	16%
Established a business risk inventory	18	Identified key metrics to report on risk	14	Annual budget process	16
Aligned BU risks with objectives	15	Written risk policy and procedure manuals consistent across all major risk types	12	Stakeholder communications	10
Have common language for risk exposures, control activities, and monitoring efforts	15	BUs analyze risks' root cause and impact	10	Management scorecards	4
Communicated expectations for risk taking to senior managers	14	Process to integrate effects of risk types	9	Remuneration	4

Source: Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, The Conference Board Research Report, R-1363-05-R, 2005, p. 27. Data is based on a survey of management conducted by The Conference Board in 2004 on 271 companies based in North America and Europe.

- discussing the creation and assessing the quality of a training platform and other educational tools to disseminate throughout the organization a business culture prone to risk-adjusted decision making;
- conceptualizing the ERM program and commenting on its design;
- being satisfied with reporting lines, delegation of authority, and systems of accountability embedded in the designed program;
- monitoring the quality of the program implementation and execution, including significant expenditures made in relation to it; and
- providing feedback for future corrections to the program.

Although the board as a whole has an oversight role, it is unrealistic to believe that all directors may be equally involved in an effort that is highly specialized and time consuming. That is why working group members raised the following considerations while discussing **how to make it practical** for the board to be part of the corporate ERM effort.

### Conducting a preliminary analysis of corporate governance practices

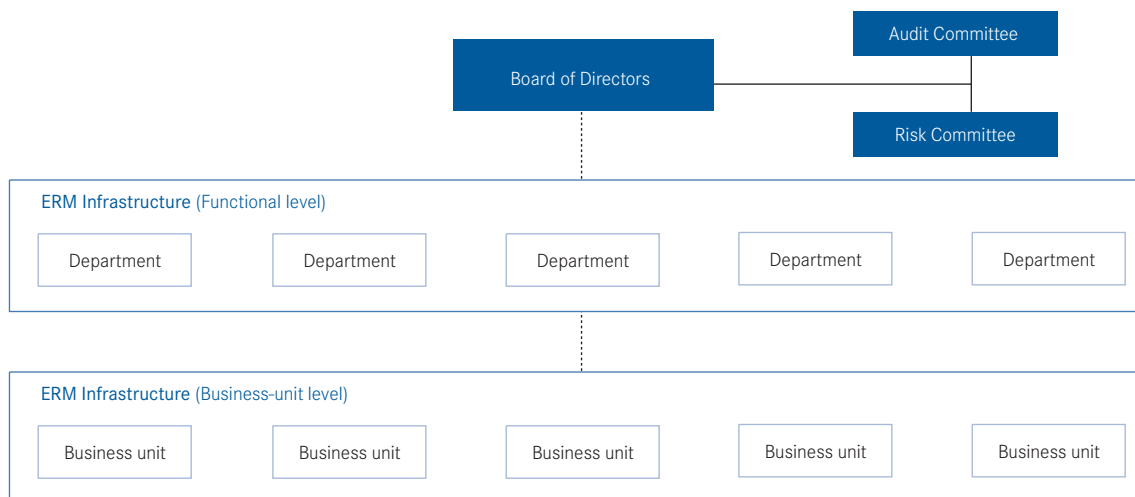
This should be done before any accountability for risk management oversight is assigned. As part of this analysis, the board should consider:

**Independence, professional expertise, and time availability of board members** Should one or more individuals be asked to take on the leadership role in organizing the board's contribution to the program, the choice should be made on the basis of board members' backgrounds and the commitment they can offer to this complex task. Independence is also crucial. Since a successful ERM process rests on the ability to reform corporate culture, it is important that the organization believes in the integrity and moral authority of their ERM leaders (at the board or any other level).

**Assignment of oversight functions to board committees** The way the board operates and fulfills its corporate governance duties should not be disrupted by the decision to get started with ERM. A contribution to the

Exhibit 3

#### The Role of the Corporate Board in the ERM Infrastructure



program from the audit committee seems to be required by NYSE standards for listed companies, and its involvement may also be justified by the expertise developed by audit committee members in overseeing those financial risk management procedures that have been developed under Section 404 of the Sarbanes-Oxley Act.<sup>41</sup> In many regards, therefore, the audit committee can act as a “catalyst” for ERM program development. Nonetheless, the board should be sensitive to the issue of possibly overloading the agenda of the audit committee and consider the assignment of certain risk oversight functions to other committees (or even the formation of a dedicated risk committee).<sup>42</sup>

#### **Quality of the information flow between board members and management**

Corporate governance standards assign a monitoring role to the board of directors, the effectiveness of which depends on the flow of information from and to management. When deciding upon the internal assignment of ERM oversight responsibilities, the board should determine risk reporting needs within the board and its committee and assess how existing reporting lines are functioning. If the board feels it necessary to facilitate the information flow, it should consider designating a committee or an independent board member to act as the interface with senior management on risk oversight.

#### **Integrating ERM oversight into strategy-setting activities<sup>43</sup>**

In positioning itself as part of the ERM infrastructure, the board should pay specific attention to the interplay between risk analysis and the strategic decision-making process. Long-term strategic choices are discussed at the board level and agreed on with leading executives, who are then entrusted with strategy implementation. This process is very delicate because the board must ensure that no self-dealing or other conflicting interest prevails over the interest of the corporation and its shareholders. Strict corporate governance standards have been adopted over the last few years to guarantee the strategy-setting process’s objectivity and integrity; it is important that, in integrating new protocols with the existing process, the board does not alter the delicate balance established by those standards. In particular, working group members discussed two aspects of such an integration:

#### **Disclosure and transparency procedures**

Risk oversight at the board level should be designed so that it fits into, and does not interfere with, disclosure procedures already in place at the organization. In fact, ERM is supposed to improve those procedures and enhance business reporting to shareholders with a clearer view of long-term strategic goals.<sup>44</sup> Should a company separate disclosure oversight from risk oversight and assign them to two separate committees (i.e., the governance committee and the risk committee), their charters should contemplate a close coordination of their activities.

<sup>41</sup> See “The Legal Foundation of Enterprise Risk Management” on p. 21.

<sup>42</sup> See “Where Boards Assign Risk Oversight” on p. 34.

<sup>43</sup> Research conducted by The Conference Board on corporate directors indicates that they are particularly concerned about the integration of risk oversight with other governance functions. See Brancato et al., *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, p. 28.

<sup>44</sup> See “Enhancing Public Disclosure through ERM” on p. 83.

## Where Boards Assign Risk Oversight

Research conducted by The Conference Board on the role of U.S. corporate boards of directors in risk management showed that two-thirds of companies currently delegate risk oversight responsibilities solely to the **audit committee**. A number of alternative solutions are also emerging, including the formation of a separate, dedicated **risk committee**. Companies that have established such committees include:

- Wachovia Corporation (risk committee);
- Citigroup, Inc. (audit and risk management committees);
- Duke Energy Corporation (finance and risk management committee);
- St. Paul's Travelers Companies, Inc. (risk committee);
- J.P. Morgan Chase & Company (risk policy committee); and
- MCI, Inc. (risk management committee).\*

At MetLife, Inc., the insurance and financial service provider, the company has chosen to place responsibility for risk management in the hands of their **governance committee**. As Curtis H. Barnette, a member of MetLife's board, explains, the company concluded that the audit committee of a large financial enterprise subject to strict U.S. regulation should be fully deploying its resources to highly-specialized matters regarding internal auditing and financial reporting. On the other hand, board members believed that there was no reason to expand the number of board committees and that the natural correlation between risk oversight and corporate governance would justify the assignment of risk oversight functions to the existing governance committee.

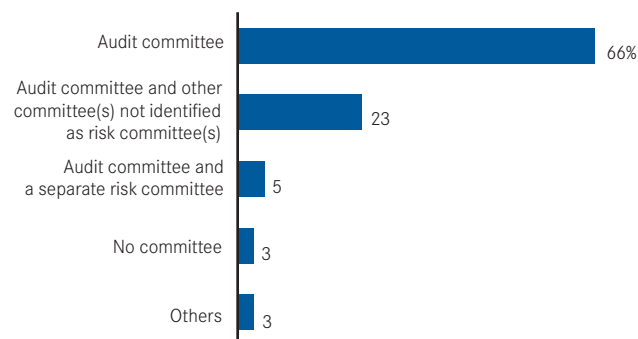
Today, MetLife's governance committee bears full responsibility for strategizing and monitoring risk management initiatives implemented by senior executives, including those initiatives taken to address financial risk exposures that are not assigned to the audit committee by federal law or regulation. Specifically, according to MetLife's Governance

Committee charter, the committee "assist(s) the board of directors with its oversight of the performance of the company's management function" by:

- "reviewing policies, practices, and procedures regarding risk assessment and management;
- receiving and reviewing reports from management of the steps it has taken to measure, monitor, and manage risk exposure in the enterprise, including financial risk (consulting in regard to such matters with independent advisors as the committee shall deem necessary or desirable);
- reviewing benchmarks for such risks and management's performance against these benchmarks; and
- receiving and reviewing reports on selected risk topics as the committee or management deems appropriate from time to time."

Although it retains ultimate responsibility for business risk oversight, the **full board** directly exercises its oversight functions in only a few of the corporations surveyed by The Conference Board. More typically, in order to facilitate a close collaboration with executives, such functions are assigned to a committee. The oversight role requires a close collaboration with executives so that the company's ability to effectively mitigate its risks and embrace new opportunities is fully understood and constantly improved. Where assigned to a subset of the board, such a role is performed more effectively and expeditiously. Also, should it not be part of their skill sets already, those dedicated directors will acquire risk management expertise and be able to offer a crucial contribution to the ERM program.

### Risk oversight is assigned to:



\* Carolyn K. Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman, *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, p. 26. This is based on a comparative analysis of Fortune 100 board committee charters.

Source: Fortune 100 board committee charter analysis conducted by The Conference Board Governance Center in January 2006.

**Compensation policies and pay-for-performance** Executive compensation is a crucial area of corporate governance as companies strive to set the right system of management incentives and find a fair correlation between pay and performance. As part of its risk oversight functions, the board should promote proper communication and alignment with the compensation committee. The committee should be aware of how the ERM infrastructure is performing and ensure that performance metrics incorporated in executive compensation schemes are appropriate to encourage the formation of a corporate culture prone to risk management. This consideration is applicable not only to the compensation of the CRO and other officers dedicated to the risk management effort, but also to business unit managers. For example, managers may be rewarded for the quality of ERM-related educational programs implemented within their business units.

## The Role of the CEO and Senior Executives

Responsibility for the conceptualization, design, and implementation of ERM begins at the top and impacts the entire organization. According to COSO's ERM framework, senior executives promote the entity's risk management philosophy and, under the auspices of the board, ensure compliance with procedures and behavioral protocols. The chief executive officer, in particular, "has ultimate ownership responsibility" for the program, including "seeing that all components of Enterprise Risk Management are in place."<sup>45</sup> Among the ERM-related executive functions performed, the CEO is in charge of:

- receiving from the board of directors the mandate to develop ERM;
- making the business case for the ERM effort and providing a firm and visible support for it;

- contributing to defining the company's risk policy, appetite, and tolerance;
- coordinating the ERM procedure design, implementation, and monitoring phases by assigning responsibilities, setting goals, and evaluating performances;
- setting the leading risk indicators (i.e., a series of quantitative and qualitative measures of risk likelihood and impact to be used within business units as part of the program);
- setting the materiality threshold (or "escalation triggers") for risk issues to be elevated through the organizational ranks;
- deciding, in accordance with a quantified risk appetite, what resources should be deployed on risk mitigation measures, how they should be allocated within the firm, and who should be responsible for their efficient use;
- being satisfied with the integration of ERM with accounting, compliance, and IT procedures;
- reporting to the corporate board on any risk issue relevant to strategy discussions; and
- ensuring that stakeholders are adequately informed (in quantitative and qualitative terms) about a long-term, risk-adjusted business strategy.

Defining the role of senior officers with respect to ERM is crucial to the success of the program. What clearly emerged from working group discussions is that senior executives in charge of risk management should be authoritative, but never authoritarian. As Scott Davenport, vice president, enterprise risk management, at Capital One Financial Corporation, stated: "The executive role in the program is to integrate risk management across the company, not to centralize it." Executive officers should frame the ERM infrastructure, set the tone for the program (i.e., a coherent risk policy, a set of effective risk metrics, clear internal reporting procedures), and assign risk ownership without expropriating from line and business unit managers their day-to-day decisions on the proper response to business uncertainties. More to the point, in ERM the executive has the role of bringing "synthesis" while leaving the "analysis" to individual risk owners.

<sup>45</sup> COSO, *Enterprise Risk Management – Integrated Framework*, Vol. 2: *Application Techniques*, Exhibit 10, p. 99.



## The emergence of the Chief Risk Officer position

The degree of the CEO's involvement in the ERM program largely depends on the decision of whether or not to assign exclusive high-level accountability for risk management to an executive risk officer. If a CRO is on staff, the CEO would still be critical for making the business case for the program and would maintain ultimate responsibility for it. Because the CEO is usually also a member of the corporate board, he or she would remain the primary interface between management and directors and would ensure that any material knowledge on risk acquired through ERM is adequately elevated to the CEO level and then communicated to the board.

A CRO would relieve the CEO of a variety of operational activities regarding the design and implementation of risk management procedures spanning the entire organization. In addition, the CRO would be responsible for articulating the ERM development effort among functional and business unit managers.<sup>46</sup> Experiences shared by working group members showed that, where present, a CRO is positioned at the very top of the ERM infrastructure

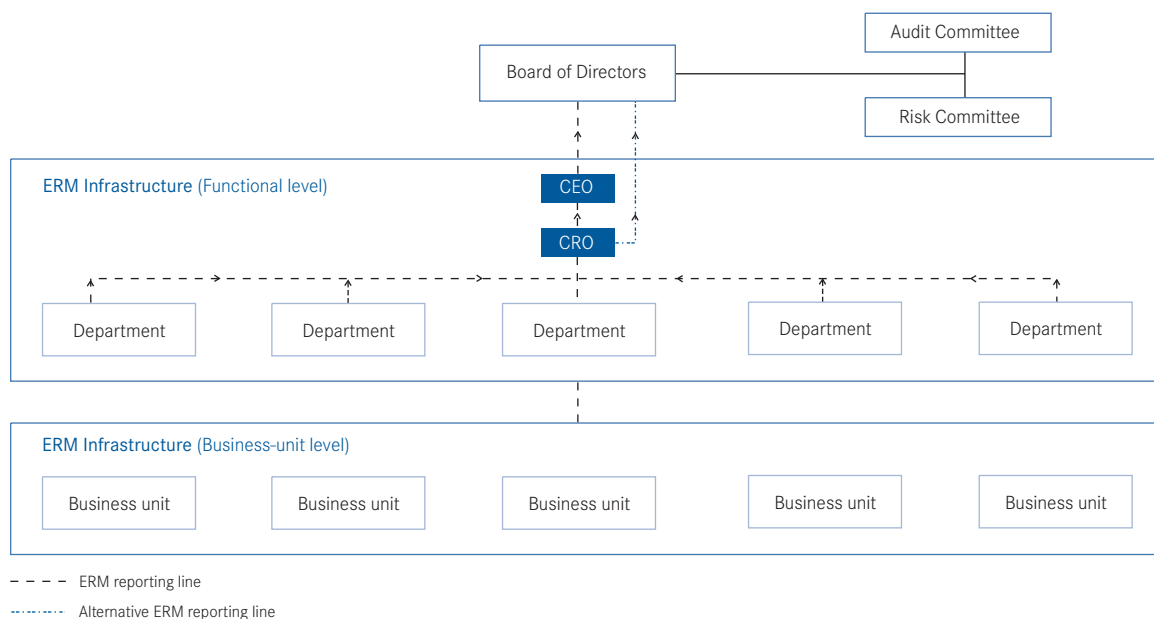
(Exhibit 4) and reports to the CEO and, in some instances, directly to the board of directors. As for CRO responsibilities, only 11 percent of responding companies participating in a 2006 survey of directors for The Conference Board report *The Role of U.S. Corporate Boards in Enterprise Risk Management* had the CRO directly inform the board on material risk issues (Chart 4).

In the last few years, a growing number of companies—especially those in the financial services, utilities, and energy industries—have been designating a specific role for their CRO.<sup>47</sup> This trend was discussed by working group members and appears to be driven by several considerations companies use to determine whether a CRO would be a valuable addition to their ERM effort:

- <sup>46</sup> Some working group corporate members use different titles for their dedicated risk executive. Other common titles include principal risk officer and executive vice president of risk management.
- <sup>47</sup> See Alasdair Ross, *The Evolving Role of the CEO*, Economist Intelligence Unit, 2005. According to the survey conducted for that report, 45 percent of companies have already appointed a CRO, while another 24 percent were looking for the right candidate for the position.

Exhibit 4

### The Role of Senior Executives in the ERM Infrastructure





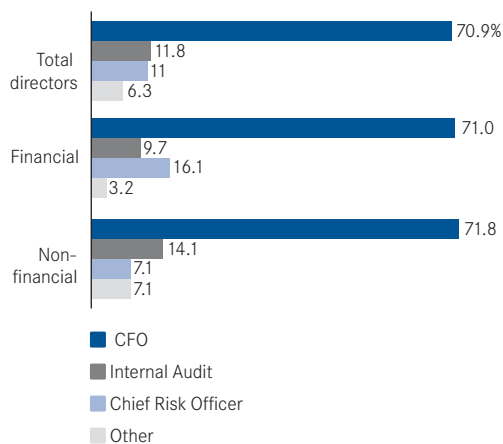
**Time availability** Especially in large, complex organizations with global operations, the CEO's **busy agenda** makes it impossible to undertake the additional commitment of implementing ERM. Even though public corporations are starting to reap the benefits of a strengthened internal control process, Sarbanes-Oxley requirements are reportedly a huge distraction for CEOs and chief financial officers (CFOs), whose schedule is currently filled with numerous time-consuming, compliance-related tasks. Corporate members of the working group suggested that the main challenge resulting from Section 302 certifications and Section 404 procedures is for CEOs and CFOs to maintain their intellectual focus on strategic, high-level decision making while complying with new regulations.<sup>48</sup> It is the responsibility of the CEO to raise this issue with the corporate board, as a senior executive dedicated exclusively to coordinate ERM may be a necessity rather than a choice.

**Skills and expertise needed** As risk management has evolved into an integrated framework, a new category of highly-specialized, highly-skilled, and highly-experienced professionals has become available in the market for corporate executives. Companies exposed to complex risk issues (i.e., utilities and energy firms) or whose business consists in managing financial products with inherent risk (i.e., banking and insurance firms) may find it more cost-efficient to hire a **specialist** than to engage a consulting firm to assist the CEO with the various stages of ERM implementation. Even though most positions are filled from within the organization, an increasing number of CROs employed by corporations in North America have substantial professional experience as risk consultants. Similarly, a growing number of candidates have earned an advanced university degree in risk management.<sup>49</sup> For example, knowledge of risk-management IT systems is one of the most valuable skills a candidate can possess.

**Visibility and authority** Working group members agree that changing the corporate culture may be the single most difficult aspect of ERM implementation. For those organizations that are less inclined to change, identifying a **central champion** or coordinator may add

Chart 4

**In addition to the CEO, who in the company is primarily responsible for informing the board on risk issues?**



Note: Percentages may not add to 100 percent due to rounding.

Source: Carolyn K. Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman, *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, The Conference Board, Research Report, R-1390-06-RR, 2006, p. 24. Data is based on a survey of 127 corporate directors based in the United States.

<sup>48</sup> Section 302 of the Sarbanes-Oxley Act requires CEOs and CFOs to issue a certification on the accuracy of financial statements. Section 404 of the Sarbanes-Oxley Act requires senior management to report on the effectiveness of internal control procedures. On these and other disclosure rules applicable to corporate executives, see Carolyn K. Brancato and Matteo Tonello, *Corporate Governance Handbook 2007: Developments in Best Practices, Compliance, and Legal Standards*, The Conference Board, forthcoming 2007. On Sarbanes-Oxley Act Section 404 implementation, also see the forthcoming report *Streamlining the Process: Current Practices and Concerns in Section 404 Compliance*, The Conference Board, 2007.

<sup>49</sup> For a study on how the risk officer figure is evolving, see Karen Thiessen, Robert E. Hoyl, and Brian M. Merkley, *A Composite Sketch of a Chief Risk Officer*, The Conference Board of Canada, 2001, p. 3.

visibility and impetus to the project. A CRO's authority in his or her field allows him or her to embody the importance that the board of directors and senior executives assign to ERM. In addition, the CRO's dedicated role may include taking the time to adequately communicate the ERM philosophy to individual risk owners and managers in the organization, ensuring that they fully understand the holistic nature of the project and do not perceive it as a threat to their own careers.

### Dissenting opinions on the need for a CRO

Some working group participants remained skeptical about how a CRO would benefit their business in the long run. Before assigning senior-level functions to a new, dedicated officer, they would rather wait for a clearer indication that there is a value proposition for integrating risk management at their companies. It should also be noted that all of the described reasons for hiring a CRO seem to be related to the extra effort necessary to get started with the ERM program; over time, as ERM becomes fully integrated with business operations, a number of responsibilities now borne by senior executives might be transferable to business unit managers or other risk owners. Although the company would still need a central authority to exercise high-level monitoring and to communicate with the board, with time, the need for a dedicated risk officer may decline.<sup>50</sup>

### The role of the Chief Financial Officer and the Internal Auditor

Of directors surveyed for a 2006 report from The Conference Board, 71 percent indicate that the CFO is, in addition to the CEO, primarily responsible for informing the board on risk management.<sup>51</sup> It is worth observing that this finding reinforces the notion that most directors are still equating business risk with financial risk, thereby missing the holistic component of ERM. As companies move toward an integrated risk management environment, awareness about the importance of a business risk reporting line is expected to increase. Consequently, the CEO, along with the CRO, should be seen as the main information channel for keeping the board abreast of what organizations learn from their day-to-day responses to risk.

This is not to say that CFOs should be excluded from the ERM infrastructure. On the contrary, working group members underscored the contribution that a CFO, together with the head of internal audit, may provide to the design and implementation of ERM procedures. Today, CFOs are not only very knowledgeable about the variety of risks affecting physical and financial assets on the balance sheet, but also experienced in how to integrate isolated responses to those risks into a cohesive, enterprise-wide process. In fact, auditing standards enacted by the Public Company Accounting Oversight Board (PCAOB) since 2004 have also been used by CFOs and internal auditors as guidelines to establish those organizational procedures on financial reporting that are now required under Sarbanes-Oxley Act Section 404.<sup>52</sup> Such procedures have a narrower focus (as they look at financial risk only) but share certain aspects—in their company-wide scope and nature—with ERM. In order to oversee their establishment, CFOs had to resolve

<sup>50</sup> See also the case study discussed in Tom Aabo, John R. S. Fraser, and Betty J. Simkins, "The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One," *Journal of Applied Corporate Finance*, Volume 17, Number 3, 2005, pp. 62–75. In the article, the authors explain "how ERM has become such an integral and successful part of Hydro One's culture that the chief risk officer may now be becoming redundant."

<sup>51</sup> Brancato et al., *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, p. 24.

<sup>52</sup> In particular, see PCAOB Standard No. 2 ("An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements"), which was approved by the U.S. Securities and Exchange Commission on June 17, 2004.

a number of issues regarding corporate culture and the firm structure, and learn how to bring together formerly fragmented solutions to financial risk that had been adopted previously by functional and business unit managers. The knowledge and experience developed by CFOs are therefore invaluable and should be transferred to the senior executive in charge of designing and implementing the integrated risk management program.

To facilitate this contribution of knowledge by the CFO and the internal auditor, the CEO may suggest that they participate in the workings of the ERM Executive Committee.

### The role of the ERM Executive Committee

The COSO framework indicates that, in some large organizations, the CEO may consider establishing an Enterprise Risk Management Executive Committee “consisting of a subset of senior management, including functional managers such as the CFO, chief audit executive, chief information officer, and others.”<sup>53</sup> The framework also enlists a number of functions assignable to a specialized committee at the executive level. Since the list includes various responsibilities already described with respect to the roles of CEOs and CROs in ERM, companies may wish to consider whether such a committee is really needed and what its interplay in the ERM infrastructure should be.

What emerged from working group discussion is that an executive committee would benefit the company if it becomes the arena where members of senior management may:

- contribute any knowledge of the business risks they own;

- share their experience with respect to any segmented solutions adopted under their management;
- participate in an open debate on what ERM should be and how it should be implemented and monitored;
- coordinate any educational program intended to train business unit managers on ERM; and
- report on the quality of the communication between risk owners and functional managers or other support functions.

In other words, a specialized executive committee funnels the diverse intellectual contributions of functional managers to the CRO (or CEO, if no dedicated executive position has been created to lead the integrated risk management program).<sup>54</sup> In addition, it should be noted that functional managers work directly with business unit managers; by means of the committee, they should be able to voice at the executive level any concerns expressed by lower organizational levels. As a result of the discussions held at the committee meetings, any decision made by the executive who is ultimately responsible for ERM implementation would be informed and based on the actual knowledge of the company acquired over time by senior management as a whole.

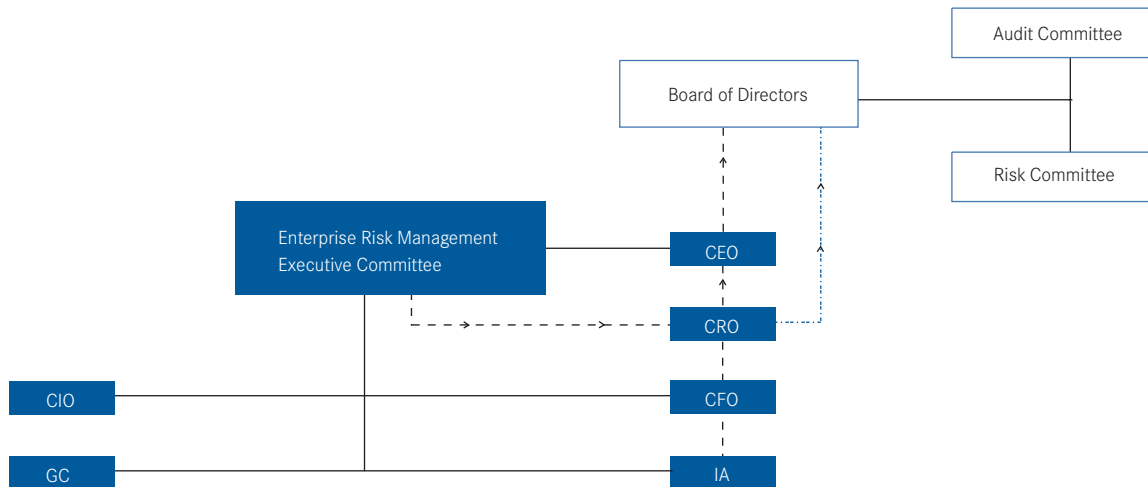
On the other hand, an organization may decide not to institute the special committee if the CEO believes that there are other venues for senior management to exchange ideas and participate in the ERM effort (i.e., where business risk is included in the agenda of periodic retreats organized for the existing executive committee). Nonetheless, as the company grows in size and complexity, the ERM Executive Committee may truly become instrumental to full-risk management integration (Exhibit 5 on page 40).

<sup>53</sup> COSO, *Enterprise Risk Management – Integrated Framework*, Exhibit 10, p. 100.

<sup>54</sup> The choice of establishing a dedicated executive committee to provide advisory support to the CEO's or CRO's ERM leadership is confirmed by survey evidence. See, for example, Tillinghast-Towers Perrin, *Enterprise Risk Management in the Insurance Industry – 2002 Benchmarking Survey Report*.

Exhibit 5

### The Role of the ERM Executive Committee in the ERM Infrastructure



--- ERM reporting line. Note that the dotted line in the schematic illustrates the reporting flow of risk management information only. It is understood that, for instance, the GC and the CFO have reporting duties to the CEO; however, such duties are irrelevant to the ERM infrastructure, as their contributions to ERM occur by means of their participation in the workings of the Enterprise Risk Management Executive Committee.

..... Alternative ERM reporting line

## The Role of Business Unit Managers and Risk Owners

The COSO framework provides that “senior managers in charge of organizational units have responsibility for managing risks related to their units’ objectives.”<sup>55</sup> Among other things, business unit managers:

- cooperate with functional managers and the senior executive in charge of ERM to establish the designed risk management procedures and, to the extent that it is necessary, adapt them to the specificities of their own units;
- assume responsibility for the implementation of the program within their units;
- document and report on ERM program execution within their units;
- are held accountable for capital expenditures made in relation to the program execution within their units;
- oversee the coherent use of risk management techniques (in particular, assessment and response techniques) by any business unit employee reporting to them;
- perform and sign off on risk assessments at least annually;
- ensure that any material “downside-risk” occurrence is avoided or mitigated in a timely manner and according to the designed response strategies; and
- elevate any material “upside-risk” occurrence to higher ranks of the organizations so that its strategic impact may be appreciated (Exhibit 6).

<sup>55</sup> COSO, *Enterprise Risk Management – Integrated Framework, Vol. 2: Application Techniques*, Exhibit 10, p. 103.

Working Group members elaborated on three **corporate governance implications** of the business unit manager's role in ERM:

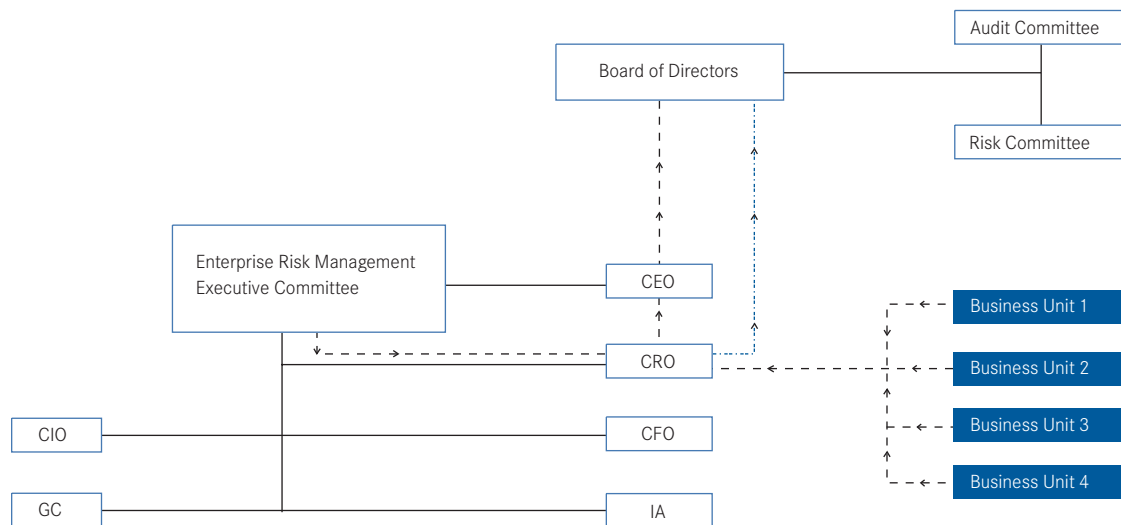
**Economies of scope** It is the responsibility of board members and senior executives to gain a full appreciation of the economies of scope achievable through risk management integration. Specifically, from their conception to their implementation, ERM procedures are supposed to enforce the proposition that related lines of business sharing the same risk ownership also share resources and create opportunities for one another while eliminating conflict-of-interest situations. The role of the corporate board is to oversee the integrity of any process established to capture those opportunities, so as to ensure that senior executives, even though they design those processes, act

responsibly and in the interest of the corporation. Executives, on the other hand, should closely monitor the process.

A related issue that was of great interest to working group members was market risk. The risk of suffering a market share loss may be owned transversally by a number of business unit managers, especially in those situations where units serve the same customer base and are exposed to similar marketing or branding issues. In this specific case, ERM could achieve adequate economies of scope if market risk is assessed and mitigated (where “downside risk”) or embraced (where “upside risk”) through a coordinated procedure involving all of the business unit managers who share its ownership.

Exhibit 6

#### The Role of Business Unit Leaders in the ERM Infrastructure



--- ERM reporting line. Note that the dotted line in the schematic illustrates the reporting flow of risk management information only. It is understood that, for instance, the GC and the CFO have reporting duties to the CEO; however, such duties are irrelevant to the ERM infrastructure, as their contributions to ERM occur by means of their participation in the workings of the Enterprise Risk Management Executive Committee.

..... Alternative ERM reporting line

**Education** Proper training on ERM techniques is essential for integrating risk management and instituting the required cultural change across the organization. The topic of risk education should be fully discussed at the board level with input from the ERM Executive Committee, where present. In fact, line executives participating in the committee tend to be the most informed about how receptive business unit managers may be and what it takes to ensure that the underlying vision of ERM is fully understood and shared by them. Because of the direct relationship with unit leaders, ERM Executive Committee members are well-suited to advise the CRO on what coaching methods should be adopted (e.g., developing an ERM manual, holding risk-based workshops, establishing Intranet message boards, etc.).<sup>56</sup>

**Reporting** Ultimately, business unit managers are supposed to ensure that any risk they own is appropriately identified and assessed according to the policies and techniques provided by ERM executives. Depending on the outcome of the risk assessment, unit leaders should make a determination as to whether a risk event:

- is material for the purposes of ERM;
- has a negative impact on the business and should be effectively mitigated or avoided altogether; and
- is an “upside risk” and should be raised to the attention of senior executives and board members for its strategic potential.

Because internal communication is essential to the success of ERM, senior management should pay extra attention to the establishment of coherent reporting lines.<sup>57</sup> Risk assessment tools, risk tolerances, risk response strategies, and reporting methods should be consistent across the organization so that any information on risk management provided by a business unit leader can be analyzed and compared with what was learned from other divisions. In addition, coherent reporting lines reinforce the notion of accountability and facilitate the monitoring role assigned to the corporate board. Working group members recognized that internal transparency and accountability markedly affect the company’s ability to inculcate a common language regarding business risk.

<sup>56</sup> See “The Importance of an Educational Platform” on p. 78.

<sup>57</sup> See “Develop Effective Internal Communication and Reporting Protocols,” on p. 77.

# ERM at Work

A number of case studies were presented at working group meetings. Although there is no “one-size-fits-all” ERM process (and a large degree of variation may result from a company’s size, structure, industry, strategy, or culture), these cases may constitute a common base of practical knowledge on how such a program actually works.

Through these case studies, The Conference Board working group identified the following stages in the development and execution of an ERM program:

- 1 Appreciate the importance of enterprise risk management
- 2 Assess gaps and vulnerabilities in existing risk management solutions
- 3 Set an underlying mission and program objectives
- 4 Establish the ERM infrastructure and assign leadership
- 5 Compile a risk inventory
- 6 Select assessment techniques and define risk appetite and tolerance
- 7 Determine risk response strategies
- 8 Develop effective internal communication and reporting protocols
- 9 Monitor ERM implementation and execution

Two additional aspects of ERM implementation were identified but not elaborated upon by working group case study presenters:

- 10 Choose compensation policies and performance metrics to promote and track the pursuit of a risk-adjusted corporate strategy<sup>58</sup>
- 11 Integrate ERM with existing operational systems (i.e. IT,<sup>59</sup> accounting/budgeting/planning, internal control, Six Sigma and other quality control systems, regulatory compliance, etc.)

The lack of practical guidance on the last two aspects also emerged from The Conference Board’s 2006 survey-based research findings.<sup>60</sup> Revising performance metrics to tie them to a risk-adjusted strategy and fully integrating ERM with existing operational systems represent the most advanced (and least implemented) stages in an ERM program. Dr. Laurie Smaldone of Bristol-Myers Squibb remarks that the primary challenge for her company in the next few years of ERM adoption will be to “achieve full integration and align ERM methods to inform employees’ objectives.”

<sup>58</sup> Integrating ERM objectives with individual performance plans ensures that everyone at the company is aware of risk. For a study on the use of stock options as an incentive for the pursuit of risk mitigation activities, see Danielle Blanchard and Georges Dionne, “Risk Management and Corporate Governance,” HEC Montreal Risk Management Chair Working Paper No. 03-04, September 2003. The study documents that (a) risk management policies can give rise to conflicts of interest between shareholders and executives when executives are remunerated in stock options, and (b) the composition of boards of directors does have an influence on risk management policies of the firm—specifically, the greater the number of external directors and the more intense the risk mitigation activities deployed by the firm. As a result, the study concludes that firms wishing to maintain their policy of remunerating executives with stock options should make sure that their boards’ risk oversight committee is reserved to competent and independent directors who hold no options to purchase the firm’s shares.

<sup>59</sup> In particular, with respect to integrating enterprise-wide risk management activities and IT, research suggests that the implementation of ERM programs is often complicated by the lack of standardized, sector-specific technological tools. The costs of developing a customized software platform may therefore limit a company’s ability to bring ERM to the most advanced stages of development. On this point, see Jerry A. Miccolis and Samir Shah, *Enterprise Risk Management: An Analytic Approach*, Tillinghast-Towers Perrin, 2000. For a review of the functionalities of ERM software applications available in the market, see *Guide to Enterprise Risk Management*, Protiviti, Inc., January 2006, p. 97.

<sup>60</sup> Brancato et al., *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, p. 19.



## ERM Case Study Companies

Risk management experts and leaders from the following companies presented case studies to The Conference Board Working Group on Enterprise Risk Management.



### Bristol-Myers Squibb

A worldwide pharmaceutical and related healthcare product company, Bristol-Myers Squibb Company (Bristol-Myers Squibb) has three business segments: pharmaceuticals, nutritionals, and other healthcare. Bristol-Myers Squibb's strategy consists of continuing support for its growth drivers, aligning sales and marketing emphasis on specialists, implementing initiatives designed to achieve and maintain a more efficient cost base, and focusing its R&D on pharmaceutical products in disease areas with significant unmet medical needs. Dr. Laurie Smaldone is Vice President, Strategy and Issues Management at Bristol-Myers Squibb and leads the enterprise risk management program.

### CapitalOne®

Ranked among the "100 fastest growing companies" by Fortune magazine, Capital One Financial Corporation (Capital One) is a leading diversified financial services business with \$108.4 billion in managed loans as of June 30, 2006. With operations in 9 U.S. cities, Canada, and the United Kingdom, it is the fourth-largest credit card issuer and the second-largest independent auto lender in the United States. The recipient of numerous awards for information technology innovation, customer relationship, and employee training excellence, Capital One was recognized in 2004 by *Operational Risk* magazine for its "Best Operational Risk Management Program." Scott Davenport is Vice President, Enterprise Risk Management, at Capital One.

### INTERNATIONAL PAPER

A paper, packaging, and forest product company with global operations, International Paper (IP) employs approximately 68,700 people worldwide and exports to more than 120 nations. Sales of almost \$24 billion annually are derived from businesses located primarily in the United States, Europe, Latin America, Asia-Pacific, and Canada. With approximately 6.5 million acres of land managed in the United States alone, International Paper is one of the world's largest private landowners. Carlton J. Charles is the former Associate Treasurer and Head of Enterprise Risk Management at International Paper. IP is at the conceptual stage of ERM implementation. "We are still making the business case for Enterprise Risk Management. That is, how to make money with it, not just avoid risk," says Charles. "But we are determined to correct a situation where risk is addressed by corporate silos, with a great deal of autonomy left to business units and limited senior management visibility."

## MetLife®

MetLife, Inc. (MetLife) is a leading provider of insurance and other financial services to millions of individual and institutional customers throughout the United States as well as internationally. Through its subsidiaries and affiliates, MetLife offers life insurance, annuities, automobile and homeowner's insurance, and retail banking services to individuals, as well as group insurance, reinsurance, retirement, and savings products to corporations and other institutions. Outside the United States, the MetLife companies have direct insurance operations in Asia-Pacific, Latin America, and Europe. Robin F. Lenna is the former Senior Vice President and Chief Risk Officer at MetLife.



## **Moody's Investors Service**

Moody's Investors Service is among the world's most respected, widely utilized sources for credit ratings, research, and risk analysis. In addition to its core ratings business, Moody's Investors Service publishes market-leading credit opinions, deal research, and commentary, serving more than 9,000 customer accounts at some 2,400 institutions around the globe. Credit ratings and research help investors analyze the credit risks associated with fixed-income securities. Such independent credit ratings and research also contribute to efficiencies in fixed-income markets and other obligations, such as insurance policies and derivative transactions, by providing credible and independent assessments of credit risk. (Moody's Investors Service is a subsidiary of Moody's Corporation (NYSE: MCO), which employs approximately 2,900 employees in 22 countries and had revenue of \$1.7 billion in 2005.) Charles Windeknecht is the former Director, Internal Audit, at Moody's Corporation.

# 1 Appreciate the Importance of Enterprise Risk Management

The first fundamental step in jump-starting ERM is to bring awareness of its existence, features, and potential benefits to the board and senior executive levels. Working group members agreed that it does not matter who first suggests that the organization should explore the viability of an enterprise-wide risk management program; what is necessary is that corporate directors and leading executives become knowledgeable about ERM and appreciate the value it may add to their strategic and operational decision-making process.

“Enterprise risk management is complex, and its technicalities—especially when it comes to risk assessment and quantification measurements—may discourage those who

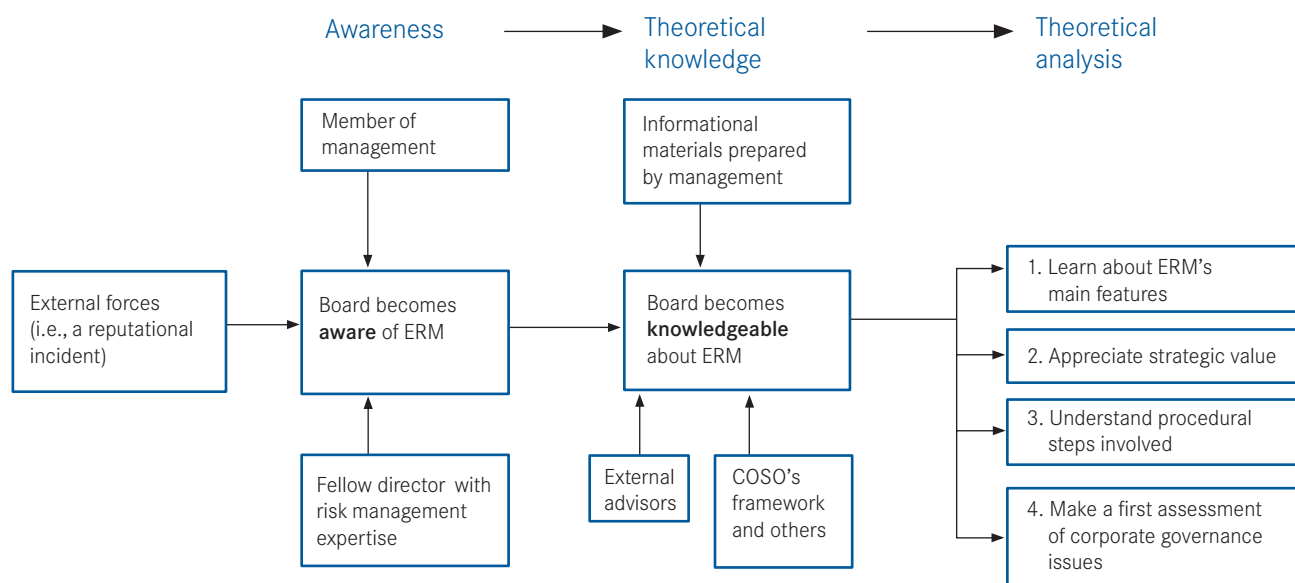
know little about this field,” says Miles Everson, a partner at PricewaterhouseCoopers and leader of PwC’s Global Risk Management group.

Should the impetus come from management, board members need to be provided with adequate informational materials on the framework. If necessary, external experts may be engaged to provide advice and knowledge to those directors who are approaching the topic for the first time. In fact, no matter where the initiative originates, the board needs to be persuaded of the business case for ERM implementation, fully embrace the effort, and set the tone for the future program, including, in particular, the corporate governance aspects of risk management.<sup>61</sup>

<sup>61</sup> See “The Role of the Corporate Board and Its Committees” on p. 31.

## STEP 1

The first fundamental step in jump-starting ERM is to bring awareness of its existence, features, and potential benefits to the board. Members of the board of directors become knowledgeable about and come to appreciate the value ERM can add to their strategic and operational decision-making process. They also make a first assessment of corporate governance issues that may arise during program implementation.



## 2 Assess Gaps and Vulnerabilities in Existing Risk Management Solutions

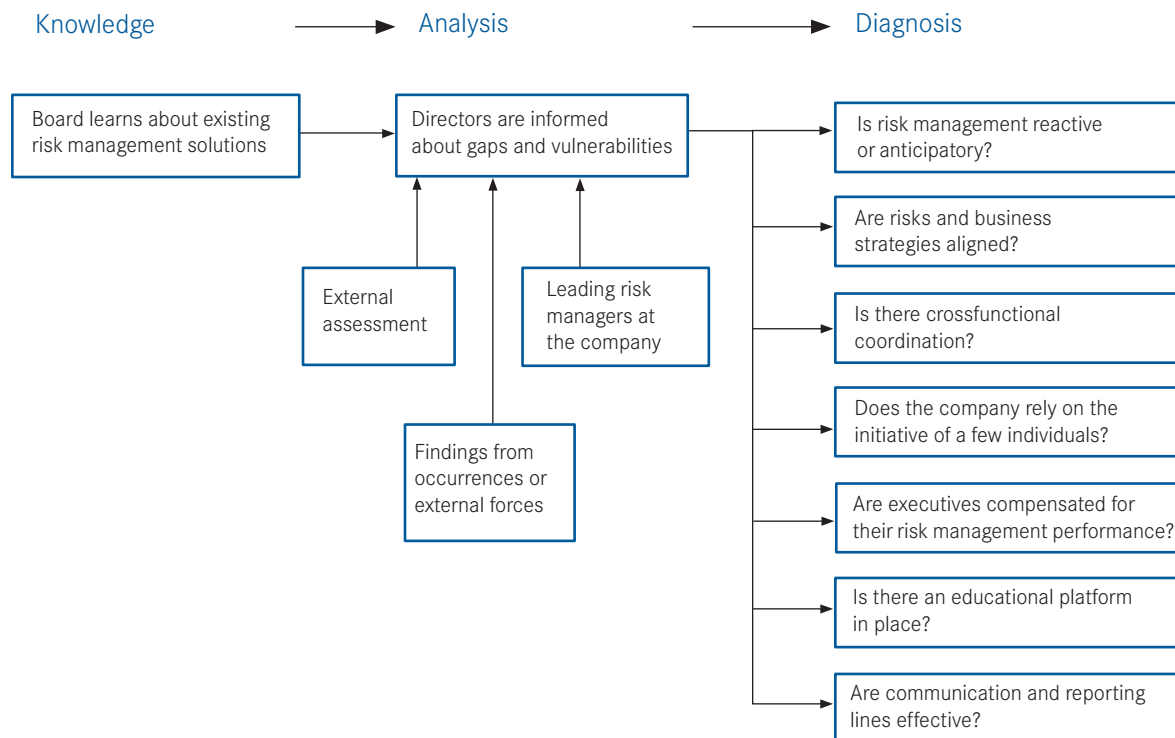
The business case for implementing ERM should rest on a detailed analysis of the limitations embedded in current risk management solutions. “The decision to jump-start enterprise risk management was taken with the full support of our board of directors, when it became apparent that our existing approach to managing risk was leaving us increasingly vulnerable,” explains a representative from a company that participated in the working group. The company was performing well with respect to managing traditional operating risks, but lacked a sustainable process to expand its view of business risk and predispose an enterprise-wide response to its occurrence.

More specifically, this company’s corporate board and senior management acknowledged that—due to a disjointed approach to risk events—the company was suffering from various **operational shortfalls**:

- On several occasions, the company had failed to anticipate events posing serious threats to the business. For example, the company fell short of its goal to achieve Sarbanes-Oxley compliance in mid-2004. The company was also ill-prepared for new international legislation that ultimately affected its cost structure.
- Critical risks were often appreciated late or by accident.

### STEP 2

The business case for implementing ERM should rest on a detailed analysis of the limitations inherent in current risk management solutions. A company may perform well with respect to managing certain repetitive occurrences, but lack a sustainable process to expand its view of business risk and predispose an enterprise-wide response strategy.



## Risk Management Weaknesses

Working group members identified a number of potential weak spots that should be discussed at the board level:

- Whether the firm has stipulated and documented risk policies and guidelines.
- Whether the firm's overall approach to risk events is reactive or anticipatory.
- Whether management seems comfortable with the alignment of business and risk strategies.
- The presence of formal risk management processes and the degree of crossfunctional coordination among them.
- The degree to which the firm's risk management effort depends upon the initiative of a few exceptional individuals.
- Whether managers are appropriately held accountable for their risk management performance.
- Whether managers are appropriately compensated for their risk management performance.
- Whether the company systematically collects and processes information on risk.
- Whether material risk reports are elevated to the top level and discussed in the context of business planning and other strategy-setting activities.
- Whether the company reviews and rationalizes the costs of its risk management activities and uses process integration as a cost-reduction tool.
- The degree of coordination and risk knowledge sharing among functional departments and business unit leaders.
- The degree of sophistication and cohesiveness of tools and techniques used to identify, assess, and respond to risk events.
- Whether management adopts capital allocation techniques to adequately support risk response strategies.
- Whether the firm has clear and streamlined internal information channels (i.e., communication and reporting) on risk management.
- The existence of an educational platform for an ongoing dialogue on risk.
- Whether the firm has a pilot risk management program tested in a specific business unit and scalable to the whole organization.
- Whether risk management activities are effectively embedded in the public disclosure process.
- The degree of sophistication of the risk management technology employed.

The participating company's "fire-fighting" response was draining resources and generating new vulnerabilities, in that investment funds had to be redirected to address operating shortfalls and human resources had to be diverted from critical functions or assignments, which ended up creating new gaps.

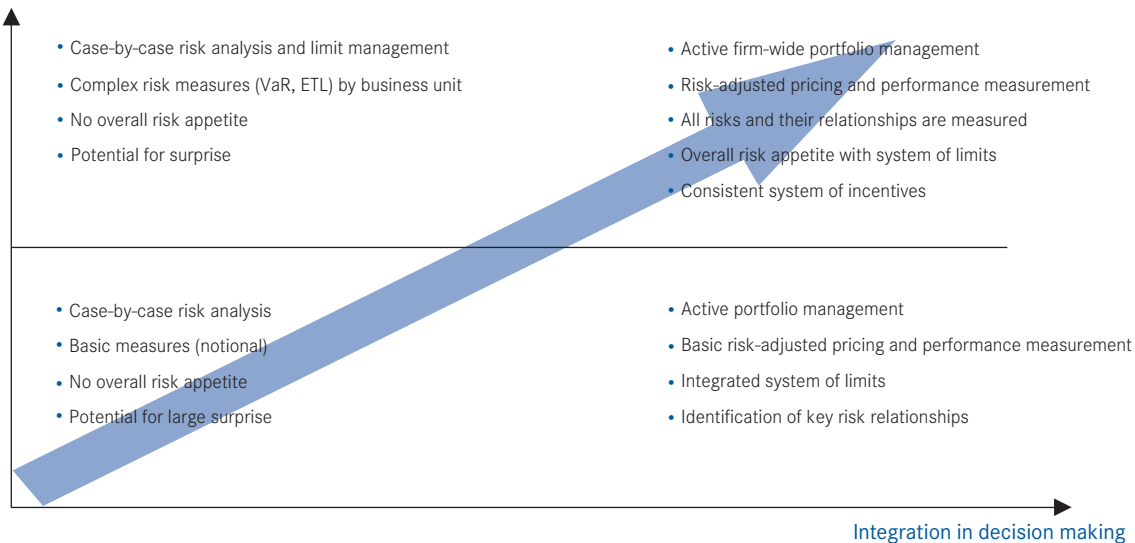
Exhibit 7, which illustrates current risk management solutions at Moody's from both a sophistication perspective and an integration perspective, may help a board assess where a company's approach to risk management stands.<sup>62</sup>

Exhibit 7

### Moody's: Assess Existing Risk Management Solutions

#### Benefits of Risk Management

##### Sophistication



Source: Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

<sup>62</sup> Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

## External influences

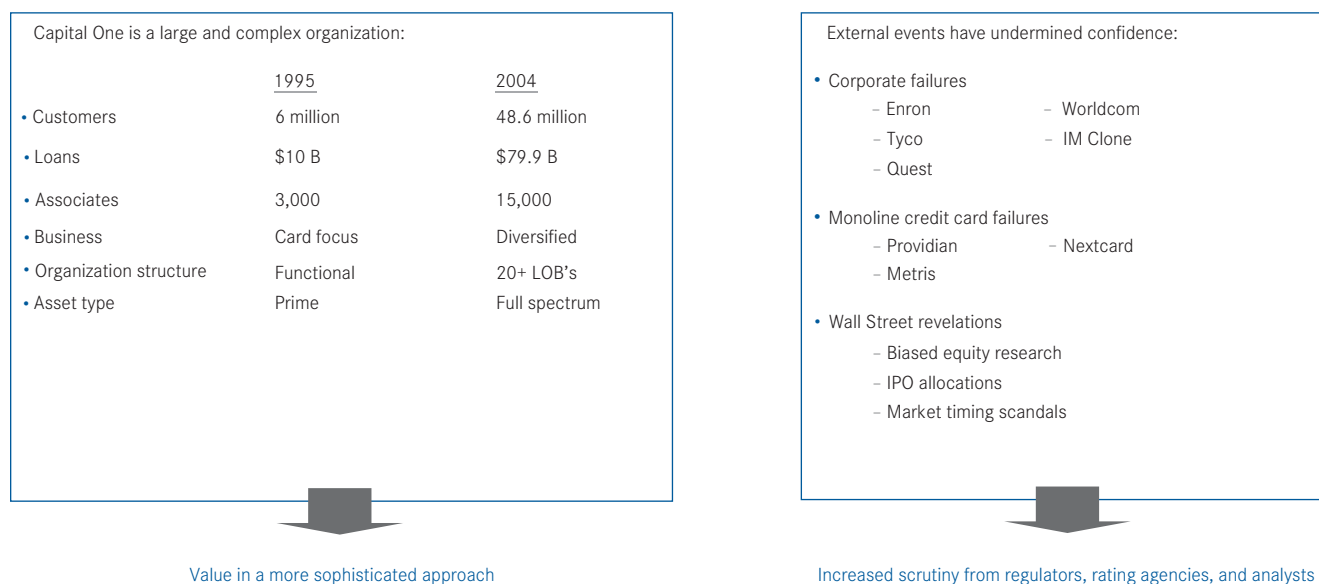
In addition to analyzing where the company currently stands with respect to risk management, in certain cases the need for integrated ERM procedures may result from a variety of **external forces**. “Because of our innovative financial business model, when we reached a certain stage of growth we encountered a significant degree of skepticism at an institutional level,” says Scott Davenport of Capital One. Therefore, the firm turned to ERM not only to effectively manage its dramatic expansion, but also to respond to the increased scrutiny on corporate governance processes exercised by regulators, rating agencies, and financial analysts (Exhibit 8).<sup>63</sup>

Similarly, Dr. Laurie Smaldone of Bristol-Myers Squibb indicates that the changing regulatory environment and issues faced by the company acted as a key driver for the initiation of the ERM program. “Because of the complexity of our business, we chose to establish a proactive framework to increase business risk awareness and promote good risk management practices,” she says. Because ERM is a work-in-progress, the process of assessing existing risk management solutions should be repeated on a regular basis as part of the program’s monitoring phase (see “Monitor ERM Implementation and Execution” on page 80).

Exhibit 8

### Capital One: Respond to External Pressures to Formalize Risk Management

The need for more formalized risk management results from internal and external forces:



Source: Scott Davenport, Capital One Financial Corporation, “Incorporating ERM Successfully,” Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

<sup>63</sup> See “The Legal Foundation of Enterprise Risk Management,” on p. 21.



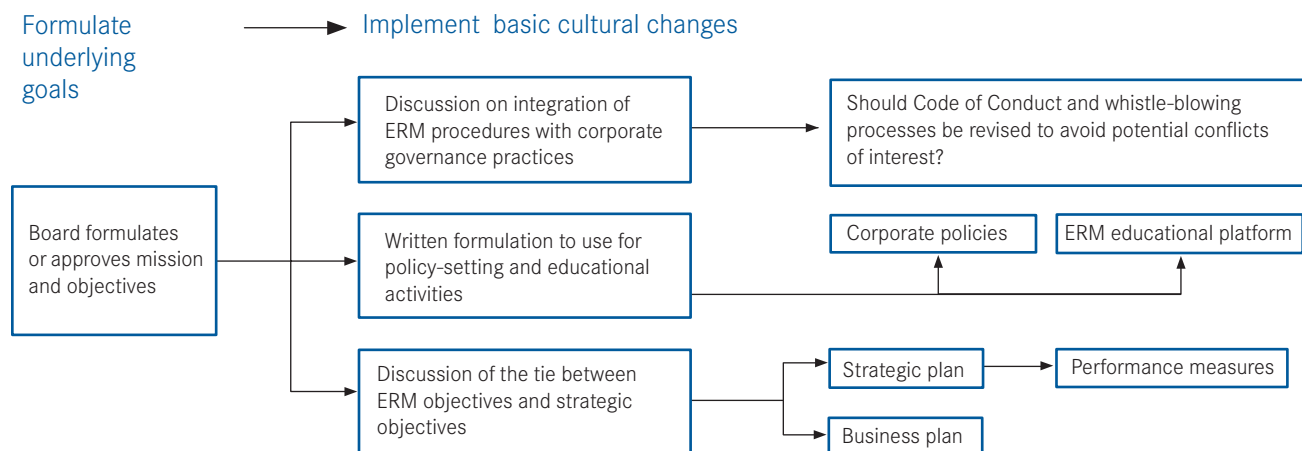
### 3 Set Underlying Mission and Program Objectives

The ERM value proposition takes center stage during this phase. Through the preliminary assessment of current risk management solutions, senior leaders may be able to appreciate the need for a comprehensive ERM infrastructure and make a solid business case to support the initiative. At this point, the business case should be formulated as a concise and effective mission statement. In addition, it should be clearly articulated in the main objectives for the program and tied to the firm's strategic objectives. While the mission statement summarizes the vision and aspirations shared by board members and senior executives with respect to ERM, the program's objectives should consist of a list of actionable goals that can be clearly communicated to the whole organization and provide a sense of purpose to the personnel involved in the effort. A thorough discussion of the benefits the company can reap from the program should constitute the foundation for drafting these documents.

Mission statements and program objectives will set the tone for the cultural change that ERM requires and are crucial for guaranteeing visibility, transparency, and integrity to the process. For these reasons, the working group recommended that board members and executive management do not overlook this preliminary step and rush to the design and implementation phases. Specifically, it was noted how corporations have invested heavily in the last few years to strengthen their corporate governance standards; it is important to avoid any disruption of those practices as the firm integrates them with new procedures and behavioral protocols. This consideration should be central to any objective-setting discussion. At the end of the discussion, board members or senior executives may suggest that the company's **code of conduct** and **whistle-blowing procedures** be upgraded to ensure that the firm is safeguarded against any conflict of interest that may arise from the assignment of new responsibilities regarding program implementation. For example, in a revised code of conduct, the ERM Executive Committee could be charged with guaranteeing the anonymity of procedures established to handle any issue raised by employees with respect to the program design and execution.

#### STEP 3

At this point, the business case for ERM should be formulated as a concise and effective mission statement and articulated in the main objectives for the program. The ERM program's objectives should be tied to the firm's strategic objectives. While the mission statement summarizes the vision shared by board members and senior executives, program objectives should consist of a list of actionable goals to communicate to the whole organization.



Companies may find it useful to document their vision of ERM in writing. One participating company described its aspiration for ERM, for example, as “to have a simple framework in place to effectively manage risks across the company while enabling growth and creating shareholder value.” The company envisioned the development of a full-fledged ERM program within a three-year timeframe and through a series of successive steps.

In the case of International Paper (IP), ERM has an even more ambitious mission, which is to facilitate a complex transformation plan through a 10-step process (Exhibits 9 and 10). At IP, the close correlation between risk and strategy set the foundation for the decision to reallocate resources and restructure the business. This case study was very useful for illustrating the strategic resonance of the program and the importance of discussing its objectives at the top level.

Exhibit 9  
International Paper: Using ERM to Foster a Transformation Plan

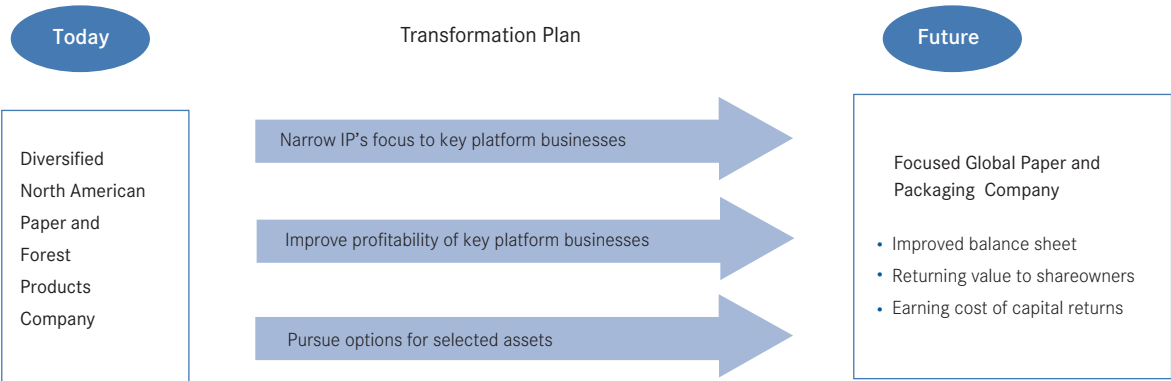
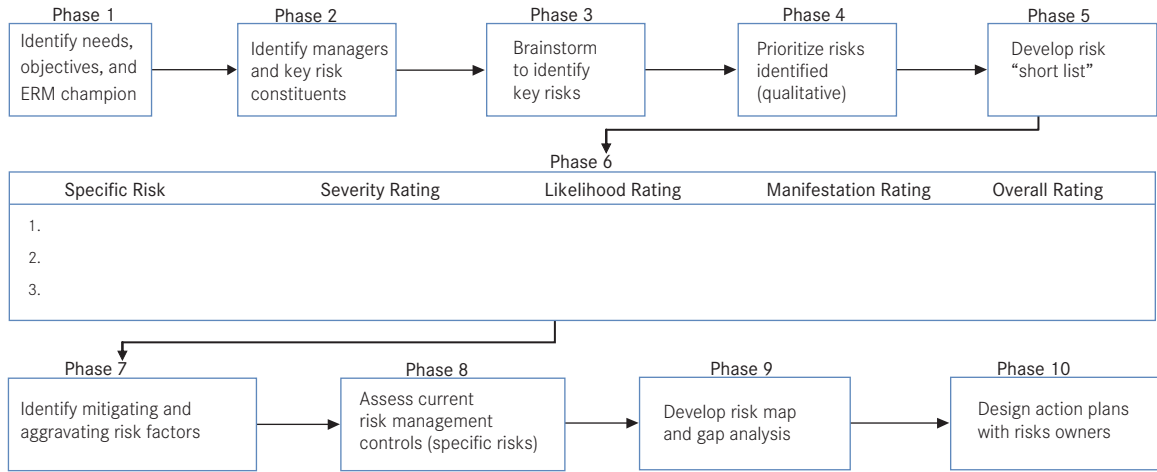


Exhibit 10  
International Paper: A 10-Phase Approach Framework



Source: Carlton J. Charles, International Paper, "Risk Management in Your Organization," Presentation to The Conference Board Research Working Group on ERM, New York, September 15, 2005.

## 4 Establish the ERM Infrastructure and Assign Leadership

Risk governance policies, executive leadership, delegations of authority, and a system of accountability should be part of the top-level discussion on the establishment of an ERM infrastructure. There was widespread agreement among working group members on the need for infrastructure design choices to be made only after a thorough diagnostic phase. As they depend on the company's size, structure, industry, strategy, and the inclinations of its personnel to accept change, such choices should be tailored to the organization and the quality of its current risk management practices.

This is how, for example, IP approached the challenge of structuring ERM. Carlton J. Charles, who formerly oversaw ERM for the company, has 17 years of experience in treasury management. "International Paper's Treasury Department was organized along traditional lines, with international treasury separate from domestic treasury. Shortly after joining IP, I realized that there was a natural break among treasury activities such as corporate finance

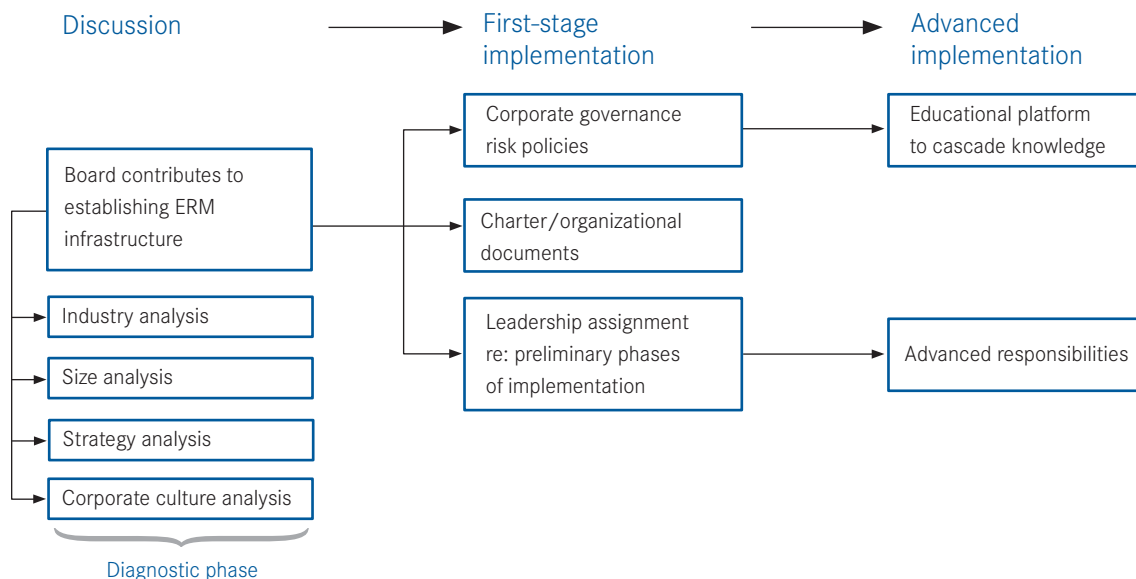
(mostly relationships with lenders and rating agencies), cash management, and risk management," Charles says. "Risk management was a major issue for International Paper because of the large currency, commodity, interest rate, and strategic risks the company faced. It made sense to reorganize Treasury in a way that acknowledged the importance of risk management to the company. That's when I decided to propose to the CFO that a separate ERM function be set up to have global responsibility for risk and that Treasury would essentially be global corporate finance and cash management." The CFO accepted the proposal and ERM initially reported directly to the CFO (it later became part of Treasury).<sup>64</sup>

Another point that emerged from the working group was that, since ERM is a work in progress, its supporting infrastructure should remain relatively flexible and open to experimentation and change. For example, when Bristol-Myers Squibb Company started its ERM effort

<sup>64</sup> Carlton J. Charles, "Risk Management in Your Organization," Presentation to The Conference Board Working Group on ERM, New York, September 15, 2005.

### STEP 4

Risk governance policies, executive leadership, delegation of authorities, and a system of accountability should be part of the top-level discussion on the establishment of an ERM infrastructure.



in 2003, it already had in place a strategy department composed of a small group of senior executives. The ERM system was embedded in the strategic planning process early in its development so there was a sustainable infrastructure to consider risk in the setting of strategy. It also enabled the ERM process to evolve and test different approaches while being tethered to strategic objectives.<sup>65</sup> Given that the strategy-setting dynamics between this small group of managers and the corporate board were under development, the role of directors in the ERM infrastructure has remained more fluid and open to the growing strategy and risk responsibilities that the executive team may take on going forward.

The case studies presented to the working group indicate that the following actions should be considered by dedicated board members and executives as part of the establishment of an ERM infrastructure:

- Stipulate corporate **risk governance policies** so as to provide full support to the ERM effort.
- Draft or revise board committee **charters** to assign ERM functions, authorities, and responsibilities to board committees, leading executives, and the ERM Executive Committee.
- **Assign leadership** of the preliminary phases of ERM implementation (i.e., compilation of a risk portfolio, selection of risk assessment techniques, definition of appetite and tolerance parameters, and any other task executed in preparation for the design of ERM procedures).

The MetLife case study exemplifies a series of actions taken to establish an ERM infrastructure. In early 2003, a risk management consulting team from McKinsey& Company was hired to assess existing risk management practices and design an ERM infrastructure.

Since early 2004, the MetLife Governance Committee has been chartered with risk oversight functions (earlier,

risk oversight was assigned to the audit committee). (For a detailed list of responsibilities, see “MetLife Governance Committee Charter.”) A new Chief Risk Officer has also been hired from outside the insurance industry. With impetus from the CRO, a risk governance framework (i.e., a set of guidelines and defined risk management responsibilities supported by the board and senior executives) has been established (Exhibit 11). An executive committee dedicated to ERM has been formed and named Enterprise Risk Council. (Exhibit 12 details the structural transition from MetLife’s historical risk management process to a more comprehensive program.)

## MetLife Governance Committee Charter

Assist the board of directors with its oversight of the performance of the company’s risk management function:

- Review policies, practices, and procedures regarding risk assessment and management.
- Receive and review reports from management of the steps it has taken to measure, monitor, and manage risk exposures in the enterprise, including financial risk (consulting in regard to such matters with independent advisors as the Committee shall deem necessary or desirable).
- Review benchmarks for such risks and management’s performance against these benchmarks.
- Receive and review reports on selected risk topics as the committee or management deems appropriate from time to time.

Source: Robin F. Lenna, MetLife, Inc., “Risk Management at MetLife: A Case Study,” Presentation to The Conference Board Research Working Group on Enterprise Risk Management, New York, January 10, 2006.

<sup>65</sup> Laurie Smaldone, “Building ERM into Strategy,” Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

Exhibit 11

## MetLife: Risk Governance Framework

Risk Governance	Risk Quantification / Aggregation / Monitoring	Risk Appetite and Control
<ul style="list-style-type: none"> <li>• Board and executive group oversight</li> <li>• Consistent standards and common risk policy</li> <li>• Independent, integrated risk management</li> </ul>	<ul style="list-style-type: none"> <li>• Common platform to aggregate risk</li> <li>• Best practice risk measurement methodologies</li> <li>• Key risk indicator reporting</li> </ul>	<ul style="list-style-type: none"> <li>• Formal process to set risk tolerance and limits</li> <li>• Risk retention and transfer strategies</li> </ul>

Exhibit 12

## MetLife: Example of a Transition to an ERM Program

<p><b>Legacy</b></p> <p>Economic Capital Methodology →</p> <p>Risk Self-Assessment →</p> <p>Operational Risk →</p>	<p><b>More Comprehensive Program</b></p> <p>Refresh economic capital methodology</p> <p>Dynamic RSCA process, “top risk” review</p> <p>Program comparable to other finance firms</p> <p><b>New</b></p> <p>All risks covered: direct vs. indirect</p> <p>Enterprise risk council coordination</p> <p>Emerging risk focus</p> <p>Specific international risk coverage</p> <p>Risk framework and standards</p> <p>Risk aggregation</p>
--	---

Source: Robin F. Lenna, MetLife, Inc., “Risk Management at MetLife: A Case Study,” Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

## Moody's ERM Executive Committee Charter and Structure

The following is the charter of Moody's Executive Risk Committee (an executive-level committee dedicated to ERM):

### 1 Purpose

"The [Executive] Risk Committee's primary purpose is to perform centralized oversight, policy-setting, information gathering, and communication to executive management and the Board of Directors, regarding Moody's important risks and its related risk management activities. In addition, the Committee shall assist the Board of Directors in fulfilling its oversight responsibilities related to the company's risk assessment and management processes.

### 2 Responsibilities

"The [Executive] Risk Committee shall be responsible for the following activities:

- (a) Identify and monitor important existing and emerging risks to the achievement of the company's strategic and operating objectives.
- (b) Formulate appropriate policies and monitoring and reporting frameworks to support effective management of important risks.
- (c) Review and evaluate the effectiveness of management processes and action plans to address such risks.
- (d) Advise on and recommend to executive management any significant actions or initiatives that the Committee believes necessary to effectively manage risk.
- (e) Ensure that activities of discrete risk management disciplines within the company are appropriately coordinated.
- (f) Report to executive management and the Board of Directors on the status of the company's important risks and related risk management processes.

### 3 Membership and Meetings

"The Chief Executive Officer hereby resolves to establish an [Executive] Risk Committee consisting of representatives nominated by executive management from each of the company's major business units and support functions. The [Executive] Risk Committee shall have a Chair appointed by the Chief Executive Officer, who will be responsible for providing overall leadership of Committee activities and setting agendas for the Committee meetings. The [Executive] Risk Committee shall meet one month in advance of each Board of Directors' meeting and additionally when needed.

### 4 Performance and Charter

"Annually, the [Executive] Risk Committee shall perform a self-assessment including a review of the Committee membership and recommendations as to any changes thereto. In addition, the Committee shall annually review its Charter and make any recommended changes thereto."

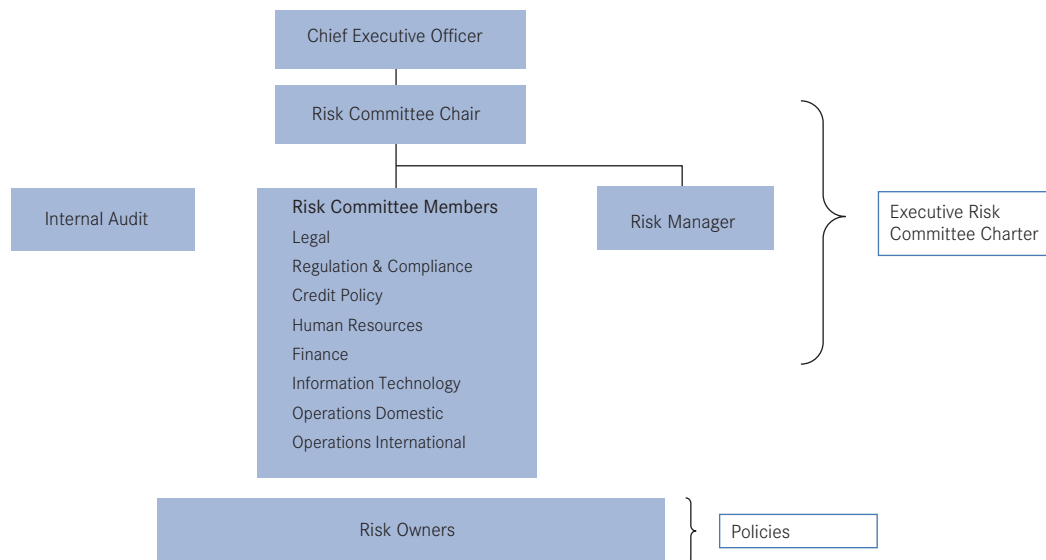
The company also reviewed and updated internal policies and governance guidelines to reflect its new risk management effort and better support the ERM initiative. Moody's board of directors worked closely with the [Executive] Risk Committee to provide general guidelines and a framework that could be used by functional managers and risk owners in the formulation of the new policies. Moody's [Executive] Risk Committee oversaw the drafting of the new documents, kept the corporate board apprised of any developments, and approved the final set of corporate policies.

As discussed previously in “The Role of the Corporate Board and Its Committees” on page 31, the role of board members should be to ensure that the quality of the internal governance regime is improved through this revision process. Internal policies are crucial to ensure that the new effort remains linked to strategy, it is implemented in a transparent manner and it is rooted in the culture of the organization.

Among the policies that were introduced or revised by Moody’s Corporation as part of the establishment of an ERM infrastructure were:

- A code of business conduct
- A conflict of interest policy
- Guidelines for core business processes
- Human resources policies and procedures
- Delegation of authority policy
- Accounting policies

#### Moody’s: Illustrative Example of ERM Executive Committee Structure



Source: Charles Windeknecht, Moody's Corporation, "Building Policy Around Key Risks," Presentation to The Conference Board Research Working Group on ERM, New York, January 10, 2006.



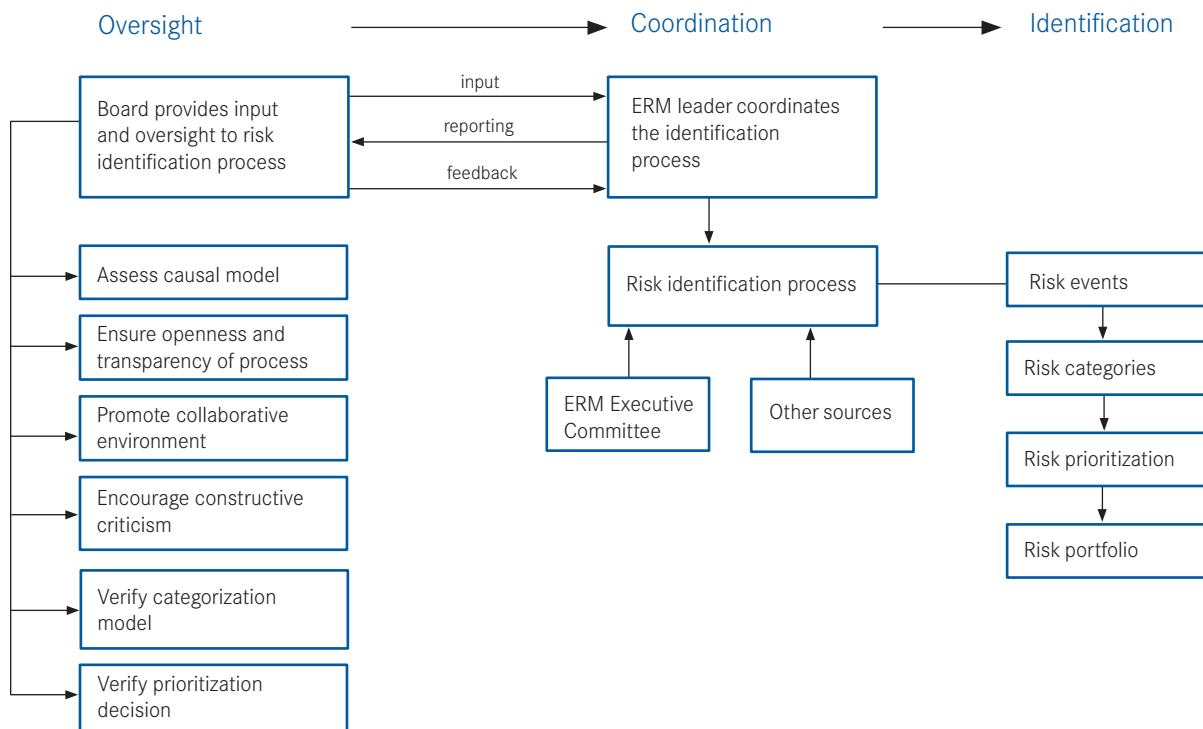
## 5 Compile a Risk Inventory

With an infrastructure in place and leadership assigned, the company is ready to work on the compilation of a risk inventory. The most important criterion used to identify risks should be the causative relationship between the event and a strategic business objective. In other words, the inventory should enlist those potential incidents that may either represent strategic opportunities or adversely affect the entity's ability to reach its long-term goals.

From a corporate governance standpoint, the important role of the board of directors in the compilation of a risk inventory cannot be overstated. In this phase, board members not only contribute their knowledge and expertise, they also oversee the process adopted by senior management to identify and prioritize risks. It should be understood that if a major risk is (accidentally or deliberately) excluded from this analysis, the rest of the ERM program will suffer a major deficiency.

### STEP 5

From a corporate governance standpoint, the role of the board of directors in the compilation of a risk inventory cannot be overstated. In this phase, board members not only contribute their knowledge and expertise, but also oversee the process adopted by senior management to identify and prioritize risks.



Since the accuracy of the risk portfolio is a precondition to the success of the whole program, the board should ensure that the process for inventorying risks is transparent and thorough. It is important for corporate directors to be aware that certain business risks may represent personal opportunities for ill-intentioned managers. In such cases, managers may have an interest in avoiding having those categories of potential events brought to the surface and addressed in a systematic and effective way. The board should therefore become familiar with any event identification technique chosen by senior executives, understand its limitations, and be able to critically analyze its outcomes. In reviewing the cause-effect analysis adopted in the process, board members should also be sensitive to the fact that, in many situations, the business is subject to the effects of interrelated events. In those cases, identification techniques should be sophisticated enough to break down and assess the single subcomponents of the causative relationship.

COSO and other ERM frameworks recommend a number of identification techniques (such as interviews, questionnaires and surveys, regulatory reviews, and facilitated workshops) that have proved effective where the risks facing the company are not immediately evident.<sup>66</sup> In addition, because of the correlation between the root causes of risk and the drivers of business success, the most common tools used in business planning (i.e., market and competitor analysis, industry benchmarking, economic forecasts, scenario analyses, geopolitical reports, quality control data, etc.) may also be deployed for the purpose of risk identification.

The Conference Board working group discussions explored the ways identification techniques were applied in practical situations. Irrespective of the technique chosen, working group members emphasized the importance of establishing a **collaborative environment** so that the accuracy and completeness of a draft risk portfolio can be tested with several constituencies in the organization. In other words, even if the company chooses to gather information on risk exposure through individual interviews or questionnaires, it is important that such information is

processed and reviewed by a dedicated team (i.e., in the form of a facilitated workshop or by convening the ERM Executive Committee). The board, in particular, should ensure that the definitive risk portfolio is truly the product of a collaborative effort and represents an enterprise-wide snapshot of the business risk facing the company.

One participating company, for example, designed a **process of meeting with senior functional and business unit leaders** to obtain their unfiltered, unedited thoughts about the corporation's risks. "We understood the need to provide an opportunity for business unit and functional managers to bring their knowledge to the table and share it with one another," a representative from the company explains. "Our process included:

- Distributing a letter to each participant setting the context for our *Getting Started* phase.
- Conducting a 'stream-of-consciousness' discussion with each leader to obtain their thoughts on the biggest risks facing the business and their suggestions regarding the timing of our efforts to address those risks.
- Sharing risk inputs from other senior leaders with each participant to stimulate thinking and obtain feedback/perspectives on the views of others."

For illustrative purposes, information obtained through this process was organized in a matrix (see Table 4 on page 60).

Based on this wide-ranging exchange of ideas, the company created a customized risk portfolio by time horizon. Items in the portfolio were first prioritized according to their timeframe. Subsequently, two general concerns (the fear of what the company does not know and could not anticipate and the possible lack of organizational capacity to tackle its risks) were added to the figurative representation of the company's risk inventory (Exhibit 13 on page 61).

Finally, risks in the portfolio were categorized as strategic (such as international vulnerability, organizational capacity insufficiency, and unsuspected competition) or operational (i.e., technology stability, fraud, and physical security) and assigned, respectively, to the senior executive/board level and to other key management leaders.

<sup>66</sup> See COSO, *Enterprise Risk Management—Integrated Framework*, p. 22.

Table 4

**An Enterprise Risk Matrix**

<i>Risks</i>	<i>Senior Leaders</i>										
	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>
Competition	+		+	+	+	+	+				+
Technology stability						+	+			+	+
Failure to use strengths	+										
Fair Credit Reporting Act	+			+	+						
What we don't know		+	+			+				+	
Virus in database/ data security		+		+	+	+					
Physical security		+									
Finance support/ the numbers		+				+				+	
Infrastructure (process and systems)		+									
Business disruption			+								
Fraud			+								
Business continuity			+								
Partnerships			+	+	+	+	+				+
Seamless operations with a changing business model			+	+	+		+				
International			+		+	+					
Deal-unique revenue recognition				+	+			+			
Organization design for a \$4B company	+		+		+		+				+

Exhibit 13

## Example of Risk Portfolio by Time Horizon

Timeframe		
Short term (2005/2006)	Mid-term (2007)	Long term (2008 & beyond)
<ul style="list-style-type: none"> <li>• Technology stability</li> <li>• Infrastructure (process and systems)</li> <li>• Business continuity</li> <li>• Deal-unique revenue recognition</li> <li>• Corruption in our data bases</li> <li>• Fraud</li> <li>• Physical security</li> <li>• International</li> </ul>	<ul style="list-style-type: none"> <li>• Fair Credit Reporting Act</li> <li>• Partnerships (revenue and vendor)</li> <li>• Seamless operations with a changing business model</li> </ul>	<ul style="list-style-type: none"> <li>• Competition from unsuspected sources</li> <li>• Organizational design for a \$4B company</li> <li>• Business disruption</li> </ul>
<ul style="list-style-type: none"> <li>• Fear of what we don't know</li> </ul>		
<ul style="list-style-type: none"> <li>• Organizational capacity to tackle risks beyond the here and now</li> </ul>		

A process similar to the one just described could lead to a long list of events with a potential impact on strategy. Therefore, a certain degree of **risk categorization** becomes necessary. Management should analyze the fundamental characteristics of each event and group them under risk categories sharing a similar nature, likelihood, geography, measurement, or response type. “The most difficult task in preparing a risk portfolio is to aggregate the risks from that long list into a maximum of 10 to 15 broader categories, because it would be impractical to develop ERM procedures for 100 risks,” says Miles Everson of PricewaterhouseCoopers.

On the other hand, it is important to remain aware that the final risk categories are made up of subcomponents, so as not to lose track of them while the ERM process continues. “The process of establishing risk categories is, per se, a form of verification of the inventory work done so far,” adds Scott Davenport of Capital One, “as it helps assure that all risks were considered and that information about significant risks from different business divisions, processes, and geographic areas can be aggregated and

reported to support our enterprise-wide risk management program.”<sup>67</sup> Also, thanks to risk categorizations, management may be able to better understand the interrelationships among risks, as well as the extent to which interdependent risks may magnify or offset each others’ effects. The outcome of such an analysis becomes particularly important when deciding on the assessment measure or response type to adopt for portfolio risks.<sup>68</sup> Working group members referred to the Protiviti Risk Model as an example of how inventoried events can be grouped in a risk portfolio.<sup>69</sup>

<sup>67</sup> See also COSO, *Enterprise Risk Management—Integrated Framework: Executive Summary*, p. 46: “Event categorization ... allows management to consider the completeness of its event identification process.” COSO also provides an example of risk categories, distinguishing between external factors and internal factors.

<sup>68</sup> See “Select Assessment Techniques” on p. 65 and “Determine Risk Response Strategies” on p. 73.

<sup>69</sup> See “A Risk Categorization Model” on p. 62.

## A Risk Categorization Model\*

Three broad but interrelated groups of events provide the basis for an enabling framework summarizing sources of uncertainty in a business.

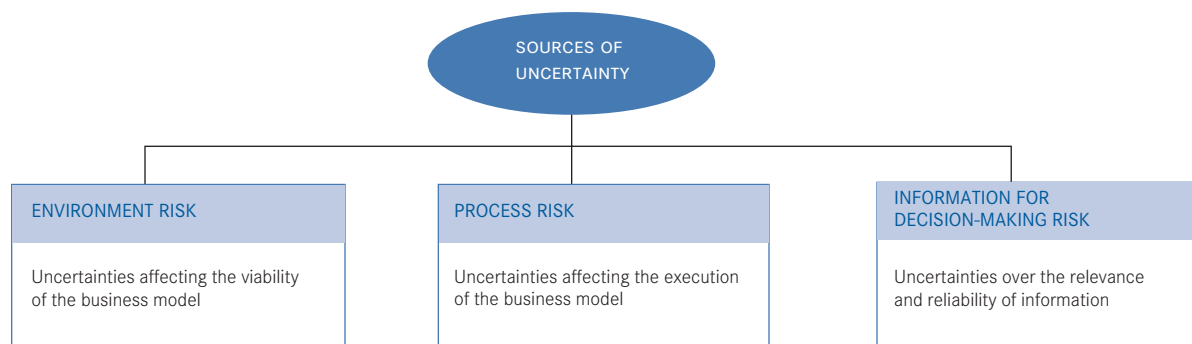
**Environment risk** includes the actions of competitors and regulators, shifts in market prices, technological innovation, changes in industry fundamentals, the availability of capital, or other factors outside the company's direct ability to control.

**Process risk** includes poorly performing corporate processes, as evidenced by the lack of alignment of management activities with business objectives and strategies, dissatisfied customers, inefficient operations, dilution of enterprise value, episodes of misappropriation or fraud, and poor employee retention.

**Information for decision-making risk** arises when information used to support business decisions is incomplete, out of date, inaccurate, late, or simply irrelevant to the decision-making process. These risks are uncertainties affecting reliability of information used to support decisions to create and protect enterprise value.

A categorization model similar to the one just described should be customized to the unique inventory compiled by the firm. The process allows companies to codify a business risk language at the strategic level, and then cascade it down to the single operating units.\*\*

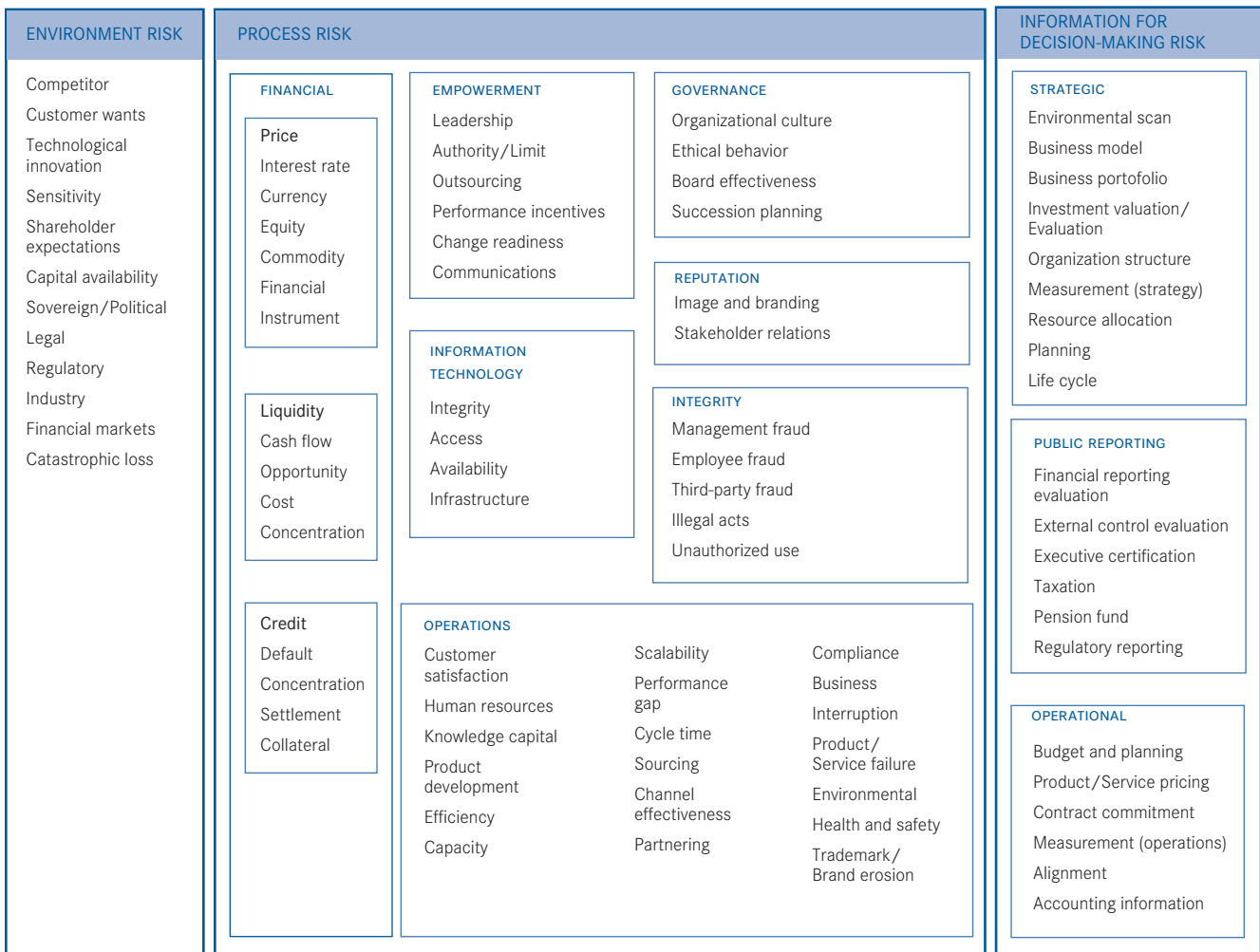
### Sources of Uncertainty



\* Adapted from *Guide to Enterprise Risk Management*, Protiviti, Inc., January 2006, pp. 53–54.

\*\* See "The Importance of an Educational Platform" on p. 78.

## The Protiviti Risk Model<sup>SM</sup>



## Corporate governance considerations for inventorying risks

A 2006 research report from The Conference Board on the role of corporate directors in ERM oversight shows that relatively few board members could point to the use of robust techniques to help them assess the quality of the risk event identification phase. Specifically, 52 percent of surveyed directors report that their boards do not have a ranking methodology for business risk factors. In addition, more than half of those that do rank key risks report that their review of such ranking occurs only annually (Chart 5).<sup>70</sup>

Members of corporate boards who are approaching their ERM oversight role may wish to consider the following corporate governance recommendations regarding their oversight of the compilation of a risk portfolio:

- As part of the strategy-setting discussion, delineate a causal model that may be used to analyze the relationship between potential events and strategic objectives as well as the interdependencies among risks.
- Be involved in the risk event identification process (at a minimum by requesting accurate reports on its progress) and ensure that it is fact-based and conducted enterprise-wide.
- Ensure that, irrespective of the technique chosen, the identification process remains open to a variety of employees with knowledge of risks facing the business (so that any geographic unit

or product unit can voice its experience and provide its feedback on the risk portfolio).

- Be critical about the outcome of event identification techniques.
- Verify the application of appropriate techniques to identify business risks related to the use of intangible corporate assets.
- Examine broader risk categories and ensure that the process of grouping similar risks is not used to exclude a relevant event from the final risk portfolio.
- Verify the rationale and accuracy of prioritization decisions and ascertain that risk rankings were not distorted to underplay the incidence of a relevant event.
- Be satisfied with the transparency of the identification procedure at each organizational level.
- Strengthen codes of conduct and the anonymity of whistle-blowing practices so as to encourage constructive criticism.

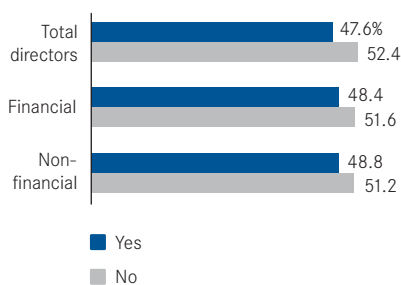
Also, risk inventories should be reviewed regularly, in connection with routine business activities and as part of the ongoing ERM monitoring operations.<sup>71</sup>

<sup>70</sup> See Brancato et al., *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, p. 22.

<sup>71</sup> See "Monitor ERM Implementation and Execution" on p. 80.

Chart 5

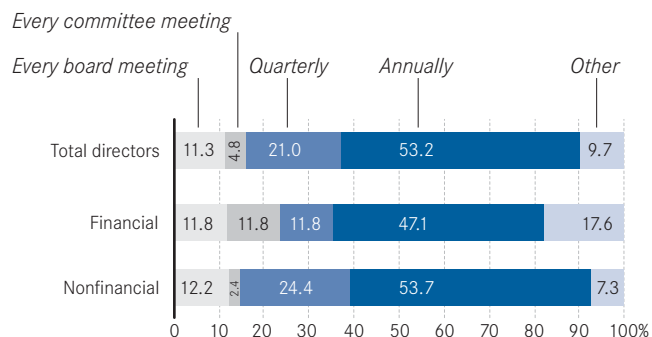
### Does the board rank key risks?



Note: Percentages may not add to 100 percent due to rounding.

Source: Carolyn K. Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman, *The Role of U.S. Corporate Boards of Directors in Enterprise Risk Management*, The Conference Board, Research Report, R-1390-06-RR, 2006, p. 22. Data is based on a survey of 127 corporate directors based in the United States.

### Except on an as-needed basis, how often does the board discuss this ranking?





## 6 Select Assessment Techniques and Define Risk Appetite and Tolerance

According to the COSO ERM framework, “risk assessment allows an entity to consider the extent to which potential events have an impact on the achievement of objectives.”<sup>72</sup> Once business risks are identified and grouped into a reasonably limited number of categories, senior management should agree upon a set of measures and techniques to assess the relevance of each item in the inventory. Functional managers, business unit leaders, and other risk owners will then be trained to utilize those measures and techniques as part of the ERM process.

The relevance of a risk event should be measured on two levels: its **likelihood** and its **impact level** (see Table 5 on page 66). In both cases, risk managers in charge of assessment may employ a variety of measures that the

COSO ERM framework describes in detail. Some of these assessment models (i.e., value at risk, cash flow at risk, earnings at risk, loss distributions, sensitivity and scenario analysis, back-testing) are quantitative and generate a numerical value that can be compared with widely-accepted benchmarks. More qualitative metrics, which are supported by numerical or statistical data (i.e., on-time product delivery data, customer satisfaction surveys, number of warranty claims filed, etc.), often translate into a narrative discussion and analysis that makes it difficult to draw comparisons within the industry or among peers.

<sup>72</sup> See COSO, *Enterprise Risk Management – Integrated Framework*, p. 33. It should be noted that other studies of risk management use a slightly different terminology and distinguish between risk quantification and risk assessment (where the latter refers to the entire process, including risk identification, categorization, prioritization, and quantification). See, for example, *Guide to Enterprise Risk Management*, Protiviti, Inc., p. 61.

### STEP 6

Once business risks are identified and grouped into a reasonably limited number of categories, senior management should agree upon a set of measures and techniques to assess the relevance of each item in the inventory. Functional managers, business unit leaders, and other risk owners will then be trained to employ those measures and techniques as part of the ERM process.

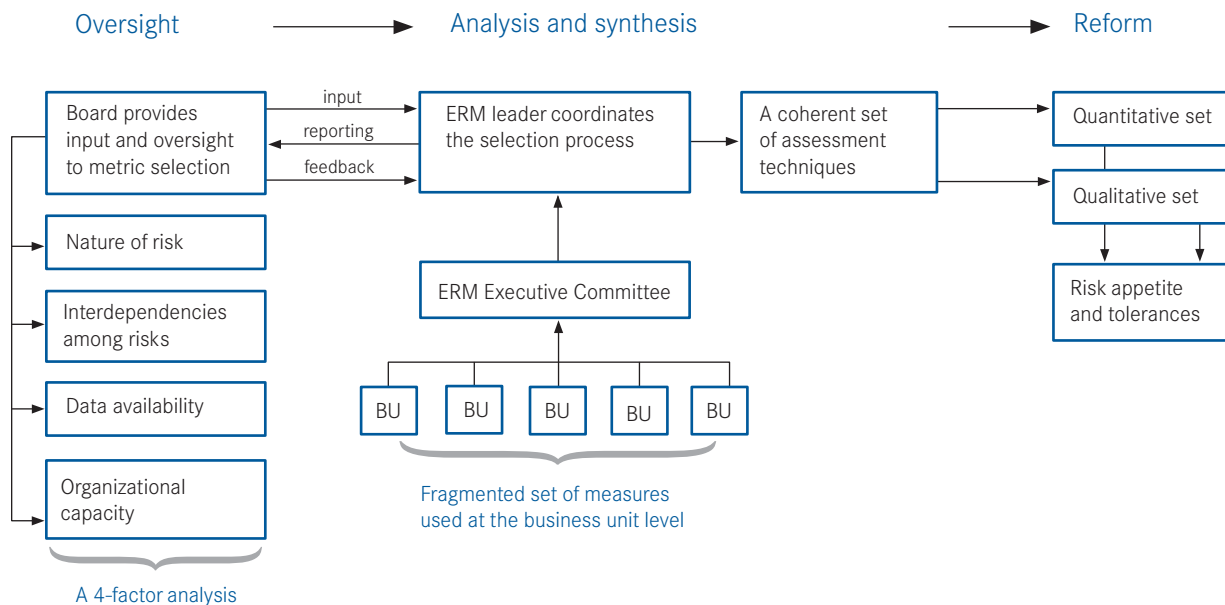


Table 5

**Techniques/Tools Used to Measure the Impact of Strategic Risks**

	Advanced ERM companies		All other companies	
	Rank	Percent	Rank	Percent
Key risk indicators	1	61%	3	31%
Individual self-assessments	2	56	4	28
Scenario analysis	3	52	1	42
Risk mapping using impact and frequency	4	50	2	34
Facilitated group self-assessments	5	48	5	25
Economic value added	6	44	5	25
Value at risk	7	33	9	17
Industry benchmarks/loss experience	8	29	7	22
Statistical analysis/probabilistic modeling	9	25	8	19

Source: Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, The Conference Board, Research Report, R-1363-05-RR, 2005, p. 37.  
Data is based on a survey conducted by The Conference Board in 2004 of 271 companies based in North America and Europe.

Working group members, however, observed that qualitative measures of risk relevance (e.g., risk maps and ranking systems) should be given a primary role in the ERM context, as they can be exceedingly appropriate to assess the upsides of risk and their potential contribution to strategic success. For this reason—and because the quality of any qualitative analysis depends on the knowledge and judgment of individuals involved and the surrounding context—the corporate board should be particularly sensitive to the integrity of the qualitative assessment process.<sup>73</sup> Specifically, the board should ensure that the organization has the processes to bring to the board’s attention any material opportunity perceived by risk owners operating at various levels of the corporate structure.

### Determining the benefits of assessment measures

In an ERM environment, senior executives should select risk measures and assessment techniques with advice and input from the board (i.e., the full board or any dedicated committee, according to the ERM infrastructure established). At a minimum, board members should request that they receive “qualified” information about the choice made by executives. “Qualified” information means that it should not only describe selected measures and techniques but should also elaborate on the rationale of the selection. Upon review of such information, board members should have an opportunity to express their concerns or disapproval.

<sup>73</sup> According to a survey of more than 1,000 directors conducted by KPMG’s Audit Committee Institute (*Spring 2006 Audit Committee Roundtable Series*), 48.5 percent of respondents point to the need for improvement of management reports regarding the potentially significant, nonquantifiable, or qualitative risks facing the company.

Through its case studies and general discussions about assessment measurements, the working group found that companies already avail themselves of a set of quantitative metrics of risk-likelihood and risk-impact. The problem is that, in a pre-ERM world, their use was somewhat fragmentary. In addition, it appears that the choice of measures was often left to the discretion of risk owners and thus lacked consistency with an enterprise-wide risk profile and philosophy. For these reasons, the enterprise risk management executive committee may provide an important input to the process of selecting a cohesive set of measures for the new program. As discussed previously, an executive committee that specializes in risk may become the arena for functional managers to contribute the in-depth knowledge of operational activities that they acquire from their direct relationship with business unit

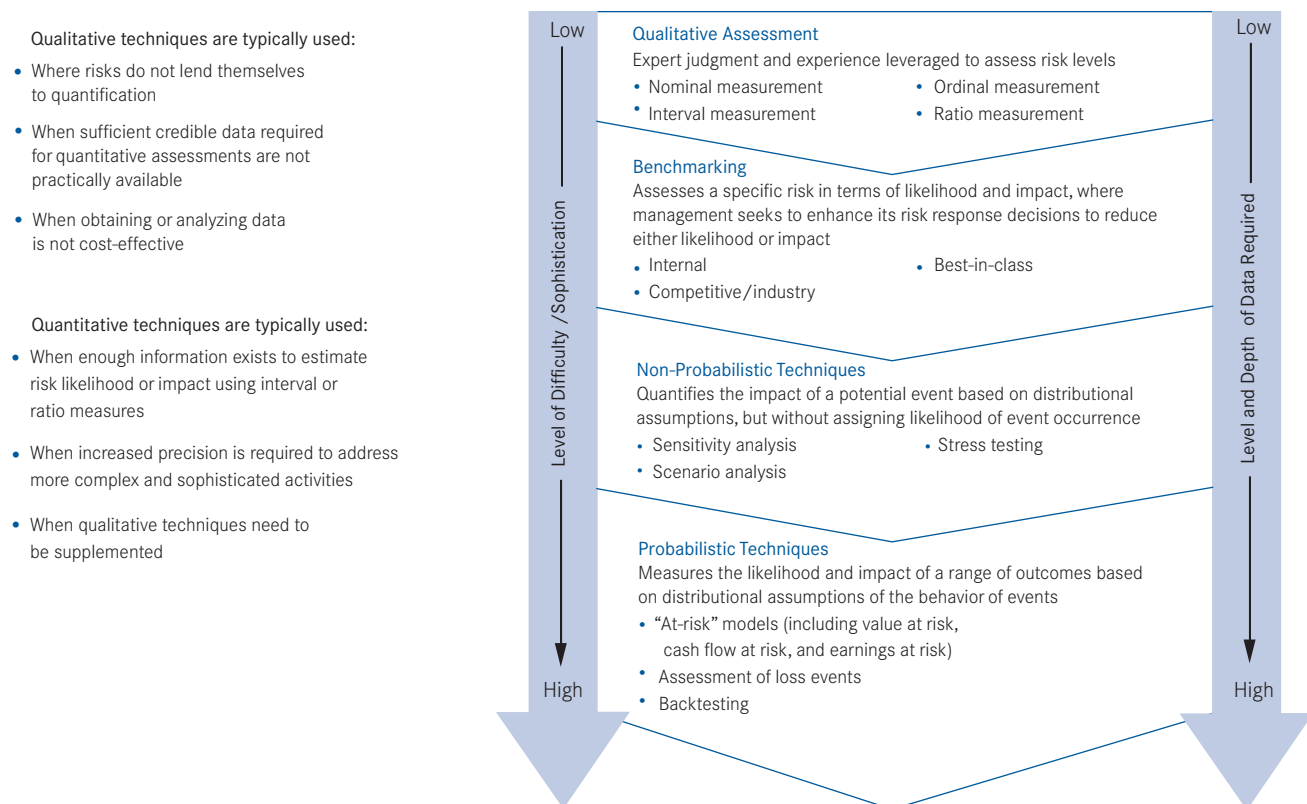
leaders and other key risk owners. By the same token, to depart from the old-style, segmented risk management approach, dedicated board members and executives should work together to ensure that the organization relies on a cohesive and balanced set of quantitative and qualitative risk assessment techniques (Exhibit 14).

Senior executives involved in the ERM program should choose risk assessment measures based on four factors, which should also be brought to the attention of the board:

**The nature of each risk in the portfolio** For example, qualitative measures appear more appropriate to assess the relevance of reputational risk or the impact of various other categories of business risk on strategic intangible assets.

Exhibit 14

### A Balanced Set of Risk Measurements



Source: Miles Everson, PricewaterhouseCoopers, "Risk Appetite," Presentation to The Conference Board Working Group on ERM, New York, September, 15, 2005.

**The possible interdependencies among risk categories** These could magnify the impact or likelihood of a series of events and require a separate, more comprehensive assessment.<sup>74</sup>

**The amount and depth of data required to apply the measure being considered** For example, the application of certain quantitative measures, such as “at-risk”

models and other probabilistic techniques based on distribution assumptions of event behaviors, may require time-consuming data gathering.

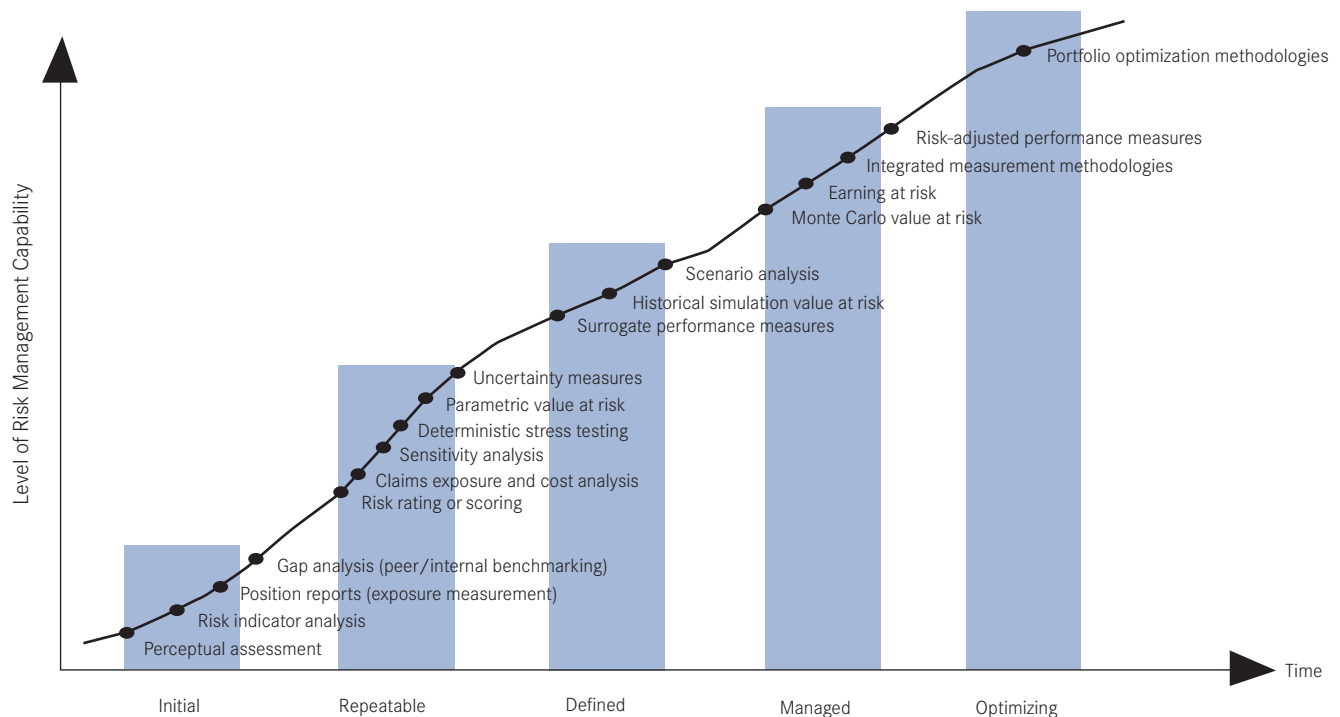
**The organizational capacity of the business unit in charge of applying a specific measure and defining the risk response** In fact, some techniques are highly sophisticated and require specific skills, which may not be present at certain organizational levels (see Exhibit 15).

<sup>74</sup> On the relationship among risk events, also see COSO, *Enterprise Risk Management – Integrated Framework*, p. 53: “Where potential events are not related, management assesses them individually. For example, a company with business units with exposure to different price fluctuations—such as pulp and foreign currency—would assess the risks separately relative to market movements. But where correlation exists between events, or events combine and interact to create significantly different probabilities or impacts, management assesses them together. While the impact of a single event might be slight, the impact of a sequence or combination of events might be more significant.”

The board of directors should ensure that the measure selection process is conducted independently and that it only reflects objective considerations on risk such as those just described. In particular, working group members underscored that in no case should the board let executive compensation issues influence the risk measure selection process. Although companies may decide to use

Exhibit 15

#### Degree of Sophistication of Risk Measures



Source: *Guide to Enterprise Risk Management*, Protoviti Inc., January 2006, p. 92

qualitative and quantitative risk data as key performance indicators (KPIs) to encourage the enhancement of their business risk management program, corporate boards should ensure that KPIs are chosen only after completing the ERM process design. In other words, KPIs should operate as incentives to achieve risk management performance goals and should not affect the selection of the tools and techniques to employ in ERM. Should management compensation be directly correlated to data on business risk before the assessment procedure has been designed, the risk measure selection process would be subject to distortions due to two conflicting interests:

The interest of the corporation (and its stakeholders) in availing itself of a set of risk assessment techniques that is commensurate with the factors described above (risk nature, interdependencies, data available, and organizational capacity).

### versus

The interest of managers to use risk measures that may underplay the impact or likelihood of a certain risk they own, therefore increasing the potential amount of the compensation for their risk management effort.

## Moody's Gold Benchmark on Risk Measurement

Moody's RMA (risk management assessment) approach uses the following "gold benchmark" to evaluate the quality of risk measurement at a company:

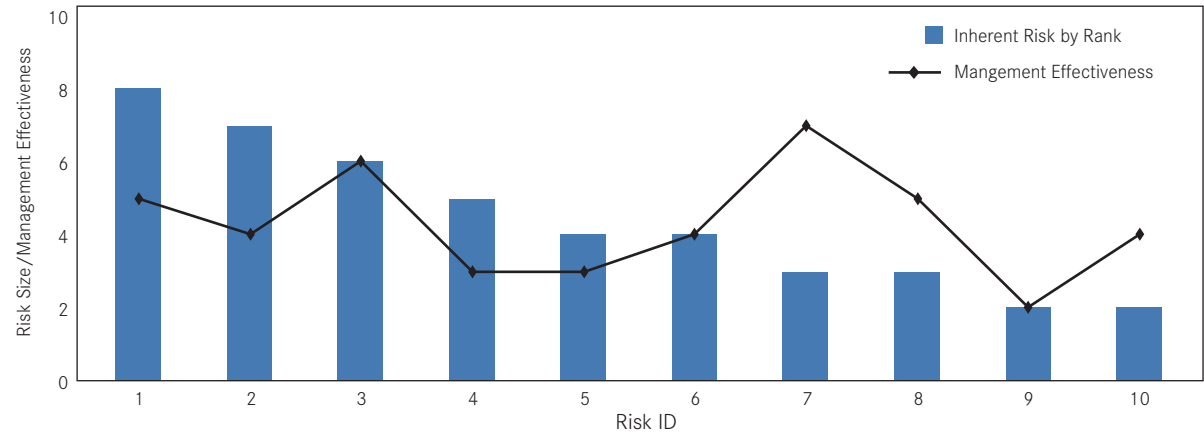
- All risks are identified and measured, even if only in a crude way.
- The firm uses a measure of total risk exposure and risk-adjusted returns, and it prices all risks.
- Risk measures are adapted to the sophistication of the organization and the types of risks taken.
- Statistical risk measures are always supplemented with stress-testing and scenario analysis.
- The leverage and liquidity dimensions are incorporated in some form in all the measures used to monitor positions and activities.
- Specialized risk measures are used to analyze one-off situations and potential structural risks.
- Failures to correctly identify or measure the order of magnitude of risks are always investigated and remediation is implemented.
- Linkages between market, credit, and liquidity risks are identified and systematically measured.
- Mark-to-Model\* exposures are systematically reviewed with model risk measures.
- A systematic independent verification of the risk analytics is used to validate the relevance and efficiency of measures.

\* Mark-to-model is an asset valuation technique and accounting methodology. As opposed to mark-to-market, it is used where no ready market is available. Instead of a market value, a hypothesis (model) is used as a benchmark in the valuation process. In this case, the technique is adopted to assess risk exposure.

Source: Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006. Also see "Rating Agency Scrutiny as an External Driver of ERM Implementation" on p. 26.

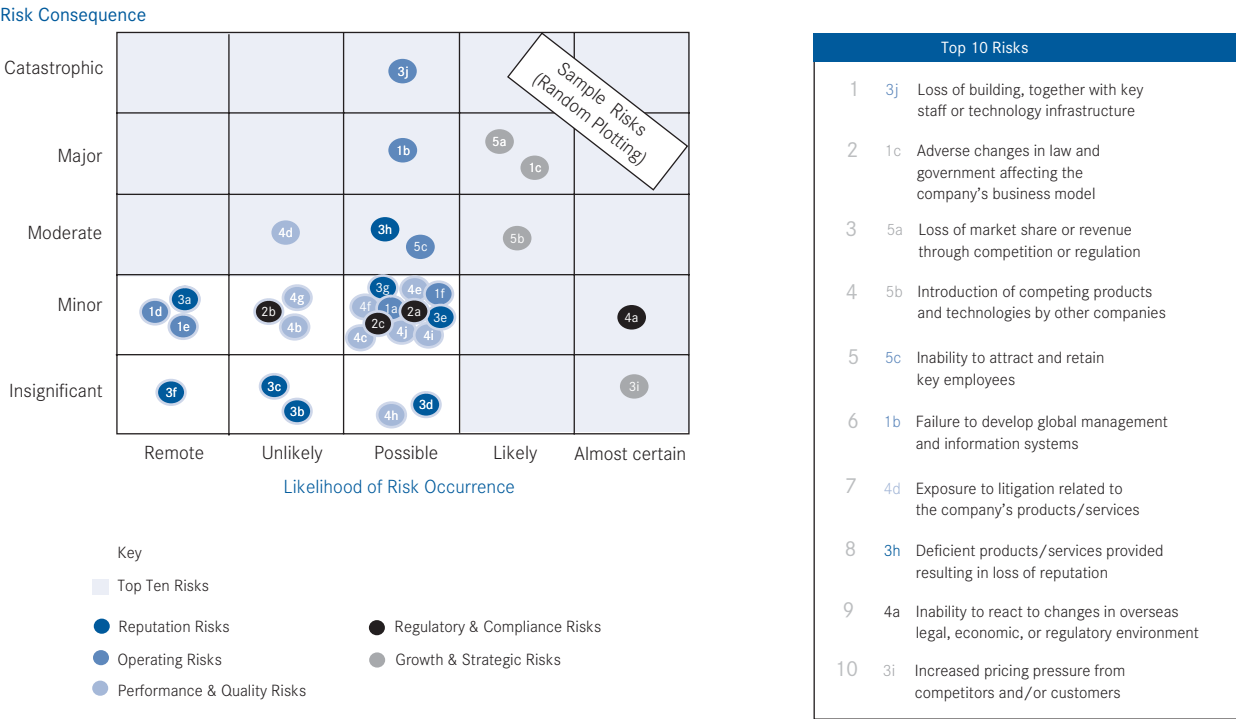
Exhibit 16  
International Paper: Risk Ranking and Gap Analysis

Categorize top 10 risks into three buckets: Optimally managed, Undermanaged, and Overmanaged



Note: Inherent risk is the risk facing an entity where no response is in place for the case of its occurrence. It differs from residual risk, which is a mitigated risk.  
Source: Carlton J. Charles, International Paper, "Risk Management in Your Organization," Presentation to The Conference Board Working Group on ERM, New York, September 15, 2005.

Exhibit 17  
Moody's: An Example of a Risk Map



Source: Charles Windeknecht, Moody's Corporation, "Building Policy around Key Risks," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

With respect to qualitative assessment, working group members stressed the need to develop a system to rate risks to organize the risk portfolio according to the degree of severity and the frequency and the immediacy of events. Specifically, it was noted that prioritizing key risks according to the level of attention that they require is also necessary to evaluate the adequacy of any **internal resources** to be deployed for the mitigation of such risks. Ultimately, the quality of the ranking system will reflect on the accuracy of any risk tolerance parameter chosen (and then periodically adjusted) by the firm.

At IP, identified risks are ranked according to their management effectiveness. In fact, this is just another way of representing a qualitative assessment of inherent risk impact, as the impact of risk on the firm's ability to achieve its strategic objectives is inversely correlated to the quality of any existing risk management practice (Exhibit 16). To represent graphically the outcome of qualitative risk metrics, executives may recommend the use of a risk map (Exhibit 17).

Risk maps and other dashboard-type reporting tools provide a portfolio-view of where business risks stand in terms of impact and likelihood; because of their schematic representation of certain meaningful business facts, they are helpful to aggregate and analyze a variety of information on risk that is difficult to quantify.<sup>75</sup> Specifically, a regular update of heat maps may simplify the top-level analysis of overall risk exposure and help ensure that it remains commensurate with the firm's risk profile. In addition, risk maps can be integrated with business planning and used to identify areas requiring the most attention at the strategic level.

## Setting levels for risk appetite and risk tolerance

Qualitative and quantitative assessment measures are also used to set the corporation's risk appetite and risk tolerance parameters. **Risk appetite** represents the broad-based, high-level view of how much risk the business is capable of undertaking in pursuit of its strategic vision; it is determined by the corporate board and senior management, at the entity level, in the strategy-setting and business planning context. The COSO framework defines risk appetite in the following manner:

The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and, in turn, influences the entity's culture and operating style. Many entities consider risk appetite qualitatively, with such categories as high, medium, or low, while others take a quantitative approach, reflecting and balancing goals for growth, return, and risk. A company with a higher risk appetite may be willing to allocate a large portion of its capital to such high-risk areas as newly emerging markets. In contrast, a company with low risk appetite might limit its short-term risk of large losses of capital by investing only in mature, stable markets.<sup>76</sup>

<sup>75</sup> For a discussion of The Conference Board's "dashboard" to track strategic measures, see Carolyn K. Brancato, *Enterprise Risk Management Systems: Beyond the Balanced Scorecard*, Research Report, E-0009-05-RR, 2005, p. 9.

<sup>76</sup> COSO, *Enterprise Risk Management – Integrated Framework*, p. 19.



**Risk tolerances**, on the other hand, are categorized by COSO as “the acceptable level of variation relative to achievement of a specific objective, and often are best measured in the same units as those used to measure the related objective.” Because risk is measured in terms of impact and likelihood, risk tolerances can indicate a variation either in risk impact or risk likelihood. Risk tolerances are used at the business-unit level and may vary from business unit to business unit according to the units’ risk exposure and the resources allocated to them to implement a risk response strategy.<sup>77</sup> Since they are correlated to the unit’s business objectives, risk tolerances are often measured using the same performance metrics adopted to track the pursuit of those business objectives.

It is the responsibility of the board to approve the firm’s risk appetite and tolerance levels as part of the annual business plan. Because of their correlation with business strategy, the board (or its committee charged with risk oversight functions) should be directly involved in the entity-level discussions intended to define the company’s appetite for risk. Specifically, board members should ensure that there is sufficient alignment among business objectives, risk appetite, and resource allocation. Although board members should not be required to participate in the determination of tolerance thresholds, they are expected to verify:

- the coherence between risk tolerances and the firm’s risk appetite;
- the adoption of an adequate set of measures to track performance at the business-unit level and ensure that it is calibrated with levels of tolerance; and
- the establishment of an adequate set of procedures to monitor the quality of risk management at the business-unit level.

Risk tolerances are an important corporate governance tool to counter the pressure that may be imposed on business managers to achieve certain strategic objectives. Such pressure may generate distorted effects and induce managers to act in a manner that is not in the best interest of the corporation and its shareholders. In this context, risk tolerances operate as limits to the profitability or productivity targets set for business managers at the executive level, ensuring that such targets remain realistic and do not encourage uncalculated risky behaviors. Board members should be fully aware of the effects of tolerance parameters when they analyze them for the purpose of approving the annual business plan.

---

<sup>77</sup> See “Determine Risk Response Strategies” on p. 73.

## 7 Determine Risk Response Strategies

Compiling a risk inventory and portfolio, selecting risk assessment techniques, and defining parameters such as risk tolerance and appetite are preconditions to the design of risk management procedures. Similar to those preliminary phases, the **design phase** is conducted at the top executive level, preferably with the leadership of a dedicated risk executive and the advisory support of the ERM Executive Committee. The purpose of the design phase is to determine the **sequence of activities** and tasks that should be performed to ensure that the company:

- responds to each event in its risk portfolio in a manner that is commensurate to the event assessment;
- monitors risk responses and other risk management issues; and
- internally reports on risk responses and other risk management issues.

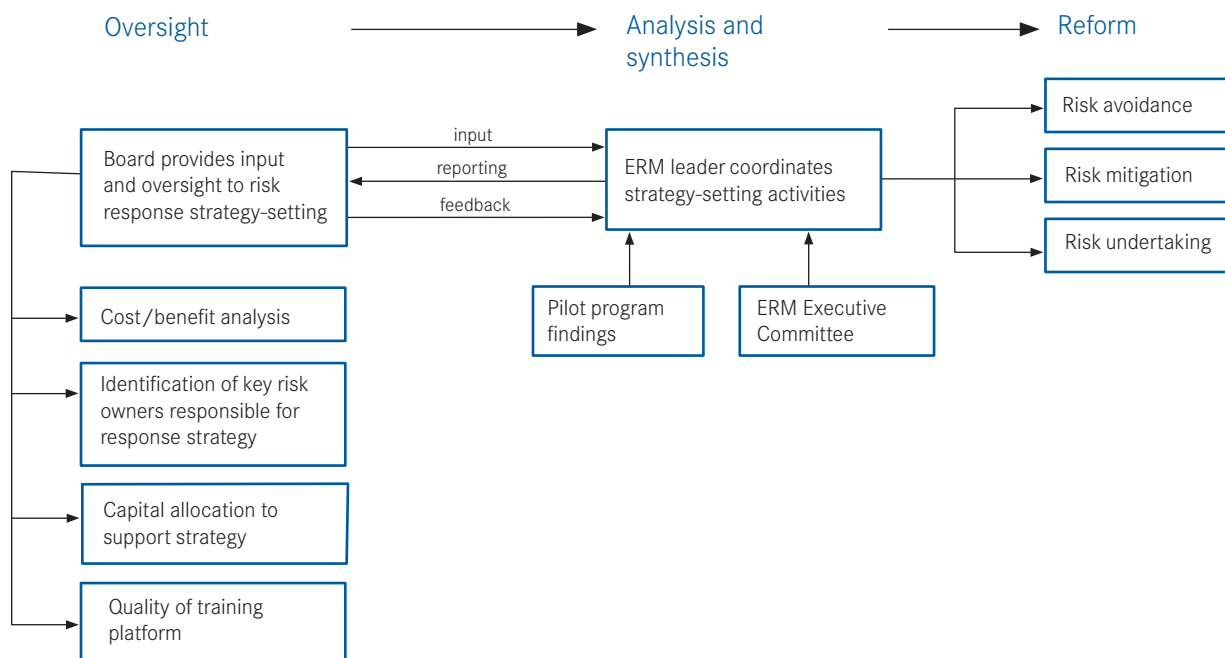
With respect to the design phase, the oversight role of the board consists of verifying that the new procedures are compatible with and do not weaken any existing corporate governance and internal control practices. More specifically, it was recommended that members of the board of directors be comfortable with:

- The **risk response strategy** chosen for each risk event in the portfolio.
- The **cost-and-benefit analysis** underlying such a choice, including a comparative analysis of alternative response choices and the evaluation of response processes already in place.<sup>78</sup>
- The **criticality** of the risk to the execution of the business model.

<sup>78</sup> For a practical example of risk response cost-benefit analysis, see COSO, *Enterprise Risk Management – Integrated Framework*, p. 59.

### STEP 7

The purpose of the procedure design phase is to determine the sequence of activities and tasks that should be performed to ensure that the company responds to each event in its risk portfolio in a manner that is commensurate to the risk assessment.



- The risk assessment **quantitative data** and **qualitative analysis** used to support a certain response-strategy decision.
- The identification—at every organizational level—of **key risk owners and leaders** who are entrusted with the implementation of risk management procedures and the application of assessment and response activities.
- The adequacy, integrity, and efficiency of any business unit **capital allocation** made to support the response.
- The soundness of **internal reporting procedures** on response implementation and residual risk.
- The quality of the **training platform** designed to coach functional and business unit managers on risk assessment, risk response implementation, and risk reporting.
- The quality of the **integration** of ERM with existing operational systems (internal control, IT, compliance, etc.).
- The soundness of procedures for **monitoring** the whole ERM program while it is executed.

Companies at the initial stage of ERM implementation may take a gradual approach to the design phase and test any proposed procedural scheme on a specific business unit or subsidiary before scaling it up across the whole organization. A detailed **pilot program** report—inclusive of observations from an initial, partial implementation and findings from the monitoring process—could be prepared for the board’s review before any decision to expand the effort is made. At Bristol-Myers Squibb, “adopting a pilot program approach was instrumental to gaining buy in from key sectors of the business and having a laboratory to test methods and develop best practice. It also gave us the time to fully communicate what we were doing and plan a phased roll-out to all business units and functions,” says Dr. Laurie Smaldone.

## Response strategy types

Determining risk responses takes center stage in the design phase, as the ultimate objective of ERM is to ensure that the organization is prepared at every level for the occurrence of events similar to the types described in the risk portfolio. Working group case studies suggest that a company may respond to an anticipated event by reducing the likelihood of its occurrence (**risk avoidance**), curbing its impact on the company’s ability to pursue business objectives (**risk mitigation**), or embracing the strategic opportunity inherent in the event (**risk undertaking**).

Because of the interrelations existing among many risk types, the best response strategy could also be a combination of these options. For example, when managing a product-safety risk (which has both a market and a reputational component), the company may wish to implement appropriate quality control processes (risk mitigation), postpone the launch of a new version of the product that has not yet been fully tested (risk avoidance), or accept any residual risk by investing in a promotional campaign focused on remaking the firm’s commitment to safety (risk undertaking).

According to COSO’s ERM framework, **inherent risk** is “the risk to an entity in the absence of any actions management might take to alter either the risk’s likelihood or impact.”<sup>79</sup> The impact and likelihood of the event can then be reassessed on a **residual risk** basis after the selected risk response has been executed (Table 6).

Risk tolerances represent the thresholds above which business units should initiate an action of avoidance or mitigation of inherent “downside risk.” Risk appetite parameters, on the other hand, suggest whether the corporation has, at the entity level, enough resources to address any residual “downside risk” or to undertake an “upside risk” and translate it into a business opportunity.

<sup>79</sup> COSO, *Enterprise Risk Management – Integrated Framework*, p. 49.

Risk owners are accountable for the response to events assigned to their area of responsibility. Nonetheless, because of the comprehensive and cohesive nature of the ERM program, their response actions should no longer be disjointed from other divisions of the firm. Instead, as the working group discussed, they should be taken according to a set of response criteria and guidelines (the “**response strategy**”) predetermined as part of the designed procedures:

- Any actual response should be aligned with the response strategy chosen as the most appropriate for that risk category. (See Exhibit 18 on page 76 for an example of such an alignment from the International Paper case study.)
- Any actual response should fully leverage existing processes (such as those that are part of the internal control network, business planning procedures, Six Sigma and other quality initiatives, compliance activities, etc.) once the intersection among related functions is fully understood.

Eventually, through a response strategy rationalization, the company should also be able to eliminate low-value, redundant internal controls.

- Any actual response should be transparent and fully reported internally. Transparency should reflect the analysis of inherent risk assessment outcomes vis-à-vis tolerance levels, the residual risk assessment outcomes vis-à-vis risk appetite parameters, and expenditures made in connection with the implementation of the response.

In particular, with respect to the cost of implementing risk response strategies at the business-unit level, working group members observed that ERM should be fully embedded in existing operational protocols and not seen as an appendage to operations. As a result, they suggested that the response guidelines should emphasize the need for business unit managers to leverage existing capabilities and limit, as much as possible, the recourse to new, dedicated human resources.

Table 6

### Examples of Risk Responses by Response Types

<i>Response Type</i>	<i>Example</i>
<b>Risk Avoidance</b>	Shelving a business project Outsourcing a complex production process
<b>Risk Mitigation</b>	Discontinuing a product after unsubstantiated indications of health hazard Canceling a promotional campaign that generated controversy Establishing a joint venture to conduct a complex production process Expanding a business insurance policy Disseminating tangible assets on different geographic regions to reduce the impact of geopolitical events
<b>Risk Undertaking</b>	Penetrating a niche market with an <i>innovative</i> product or service Entering a sponsorship agreement with an <i>emerging</i> celebrity Investing on a cutting-edge technology that may offer a future competitive advantage

Decisions taken by senior executives and ERM leaders in developing response strategies and guidelines should be supported by a thorough cost-benefit analysis and communicated to the board. Communications should also explain why alternative response strategies have been excluded. Specifically, the **cost-benefit analysis** should be tailored to each risk category in the firm's risk portfolio and may include:

- a discussion of the time horizons regarding both the impact of the risk event and the implementation of the response;
- an assessment of the resources the firm would need to deploy to implement a specific response,

including the ability to access external capital to finance the response; and

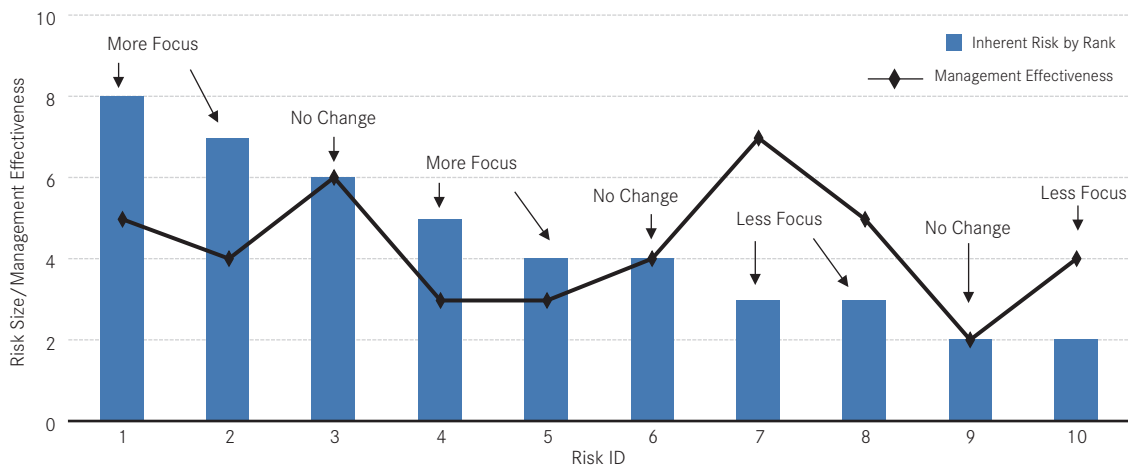
- the consistency of a response strategy with long-term business objectives.

In addition to the response guidelines, leading executives should identify as part of the ERM procedures those **response control activities** (such as approvals, authorizations, verifications, reviews of operating performance, security of assets, and segregation of duties) to which each actual response should be subject.<sup>80</sup>

<sup>80</sup> See COSO, *Enterprise Risk Management—Integrated Framework, Vol. 2: Application Techniques*, p. 63.

Exhibit 18

#### International Paper: Risk Response Strategy



Source: Carlton J. Charles, International Paper, "Risk Management in Your Organization," Presentation to The Conference Board Working Group on ERM, New York, September 15, 2005.

## 8 Develop Effective Internal Communication and Reporting Protocols

An internal flow of information is essential to the success of ERM. Therefore, in designing the program, senior management should pay extra attention to establishing coherent communication and reporting practices. Board members, for their part, should analyze the quality of internal reporting lines and be persuaded that information on risk that is material for strategic purposes will be channeled upstream and brought to their attention. In particular, working group case studies indicated that, in an organization with a number of overlapping communication systems, ERM offers the opportunity to redesign information flows, smooth asymmetries and inconsistencies, and eliminate redundancies.

The corporate board, for its part, should ensure that the communication and reporting frameworks are not over-engineered by management; simplicity and transparency are key to a streamlined system of internal information

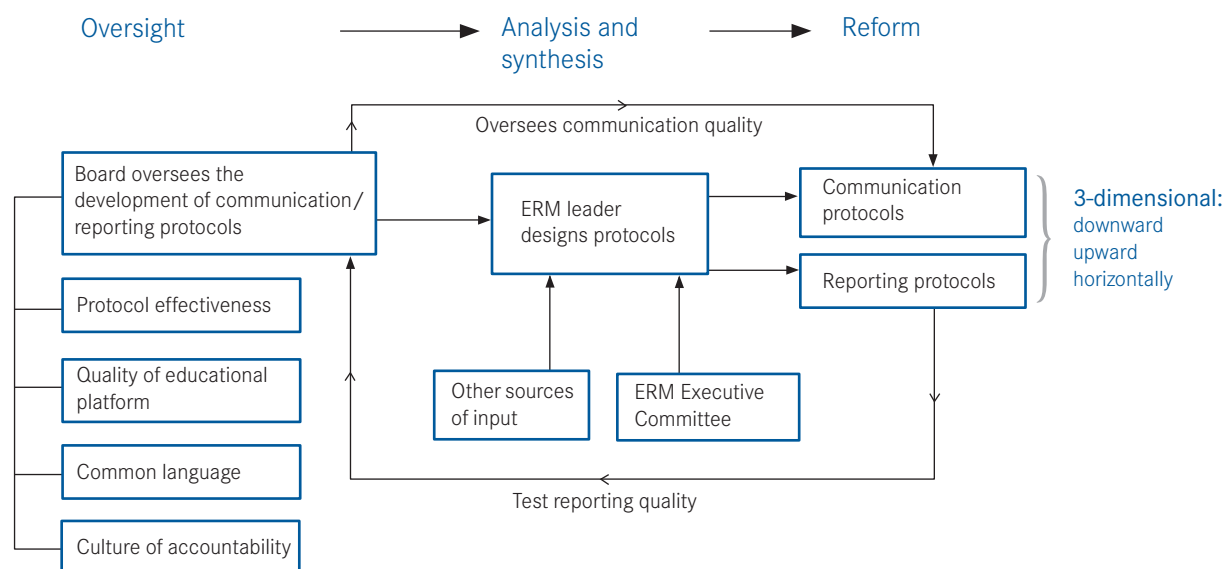
on business risk. Working group members also remarked on the need to ensure the three-dimensional functionality of the information system. Specifically, the board should verify that information flows:

- **downward** (to cascade risk management knowledge, to inculcate a renewed risk-aware culture, and to provide implementation guidance);
- **upward** (to raise risk issues, to elevate new opportunities, to provide input on the infrastructure, to provide feedback on the ongoing process, and to report irregularities); and
- **horizontally** (to ensure alignment and coherence among functional departments and operational units, to foster synergies and knowledge-sharing activities, and to encourage economies of scale).

Effective downward communication vehicles, in particular, are necessary to inculcate ERM leadership values and encourage a collaborative culture among employees. The COSO framework states, “All personnel receive a clear message from top management that enterprise risk

### STEP 8

An internal flow of information is essential to the success of ERM. In designing the program, senior management should therefore pay extra attention to establishing coherent communication and reporting practices. Board members, for their part, should analyze the quality of internal reporting lines and be persuaded that information on risk that is material for strategic purposes will be channeled upstream and brought to their attention.



management responsibilities must be taken seriously. They understand their own role in enterprise risk management, as well as how individual activities relate to the work of others.”<sup>81</sup>

Risk-portfolio categories, assessment tools, risk tolerances, and response strategies should be uniformly disseminated across the company in order to create an environment where the same language is spoken and data flowing from different organizational levels are commensurate with one another and easy to analyze comparatively. Working group members reinforced the notion that the lack of a common language impairs effective risk management and insisted on the need for a solid educational platform to support the ERM effort. By the same token, rigorous upstream reporting protocols reinforce a culture of accountability and facili-

tate the oversight and monitoring roles assigned, respectively, to the corporate board and senior executives.

The corporate board should make sure that the organization avails itself of supplemental employee communication channels to reduce any possible shortcomings of traditional reporting lines. As discussed previously, the quality of codes of conduct and the anonymity of whistleblowing programs should be assessed as part of the oversight that corporate directors exercise on ERM.<sup>82</sup>

All of the companies that participated in working group case studies indicated that they have been working on the development of detailed information technology systems to support the gathering and reporting of risk-related information throughout their organizations.

Tools Currently in Use

With respect to management reporting to the corporate board, research conducted in 2006 by The Conference Board Governance Center shows that the following are the most common risk reporting tools used:

Narrative Risk Report	50%
Dashboard-style Report	11
Slide Presentation	11
Risk and Heat Maps	7
Informational Package	7*
Discussion	4
Punch Lists	4
Other	7

\* Informational packages may be composed of a number of reporting means and include, for example, a narrative risk report, an illustrative report (dashboard-style), and descriptive materials on ERM supplied to management by the consultants engaged to assist the company with the development of the program.

Source: Carolyn K. Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman, *The Role of U.S. Corporate Boards in Enterprise Risk Management*, The Conference Board, Research Report, R-1390-06-RR, 2006. Data are based on phone or personal interviews with 30 board members from a variety of industries (including financial services, retailing, food and beverage, technology, oil and energy, transportation, equipment manufacturing, and general manufacturing). In the interviews, directors were asked to respond based on their overall board experience, not necessarily with regard to specific companies.

The importance of an educational platform

It takes years to develop the corporate culture necessary for ERM to work properly. ERM leadership values need to be disseminated throughout the organization by means of sound communication practices. Such practices should take into account that certain business units may be more eager or prepared than others to be involved in the process. “Ours is a U.S.-based company with worldwide operations. Once we made an ERM plan at the executive level,” says Dr. Laurie Smaldone of Bristol-Myers Squibb, “we realized that not everyone at the business-unit level understood the value of the new approach to risk management. Risks had been routinely managed locally so it took time and hands-on exposure for the effort to gain momentum.” An educational platform, which could be internally developed or outsourced, according to the firm size and resources, may therefore help fill the knowledge gap among divisions and ensure that everyone is on the same page.

Business-unit level risk owners should be educated on the risk vocabulary and categorizations made when the firm’s event portfolio is compiled and parameters such as risk appetite and tolerance are set. In addition, they should be guided through the ERM process scheme and trained on the use of risk measurements, the implementation of

<sup>81</sup> See COSO, *Enterprise Risk Management – Integrated Framework, Vol. 2: Application Techniques*, p. 67.

<sup>82</sup> See “The Role of the Corporate Board and Its Committees” on p. 31.



## Moody's Gold Benchmark on Risk Intelligence

Under Moody's RMA (risk management assessment) rating framework, corporate communications, internal reporting, and integration among operational systems constitute the company's "risk intelligence." The framework considers the following key benchmarking features of an optimal internal reporting system on risk:

- Requirements for risk management are seamlessly integrated in the technology platform and initiatives.
- Risk systems enable managers to access risk data quickly and from all locations.
- Risk infrastructure is optimized, minimizes the number of data sources, and has routines to clean and reconcile data inputs.
- The risk systems are completely aligned with the accounting platform, enabling full reconciliation with P&L at a very detailed level.
- Risk applications enable aggregation of all risk data across geographies, regulatory entities, risk types, and risk books.
- Risk applications enable full decomposition of risk measures down to the lowest level.
- The risk technology budget is commensurate with the objectives, the risk profile, and the sophistication of the firm.
- Risk reports are dynamic, timely, include measures and risk narratives, and are readily available.
- Risk knowledge is shared widely across the firm at all levels.
- The firm is aware of the need for public disclosures and is a leader in establishing best practices for transparency.

Source: Hervé Geny, Moody's Corporation, "Risk Management Assessments," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006. Also, see "Rating Agency Scrutiny as an External Driver of ERM Implementation" on p. 26.

selected response techniques, and the standards to report internally on risk management issues. Finally, they should make sure that any unit employee involved in the process is prepared and qualified to contribute to it. Periodic benchmarking reports, which track ERM performance of best-in-class peers and are becoming available by industry type and stage of development, may be disseminated among risk owners as part of the coaching program and used as a catalyst for improvements.

Working group members discussed the use of **educational tools** to effectively describe how assessment metrics and techniques should be applied in practice. The most common educational tools discussed were a risk glossary, a process scheme (or ERM flow chart), and an ERM application manual. "In the experience of Bristol-Myers Squibb, it was helpful to develop and maintain an ERM Manual to codify methods and educate new teams," says Smaldone. Other useful vehicles are e-mail discussion groups, Intranet message boards (blogs), and corporate newsletters: "Online technologies also seem to be helpful

in providing educational support as well as direct team training and orientation," Smaldone explains. "As risk management best practices are identified, they can easily be shared across the organization using the common language understood by all employees, at any hierarchical level." The continuity of the educational effort ensures that ERM remains an innovative, ongoing process for the corporation.

Board members and ERM executive leaders should fully value the importance of this coaching effort, as the dissemination of a common language and a cohesive business culture on risk depend on it. Larger companies, such as Bristol-Myers Squibb, have invested significantly in their ERM training platform and have formed a dedicated, six-person task force to manage it. "It is a truly global effort," says Smaldone. "We need to be conscious that the responses necessary to certain risks (especially regulatory and compliance risks, environmental and social risks, and ethical risks) may be perceived differently from country to country."

## 9 Monitor ERM Implementation and Execution

In an integrated risk management environment, any activity conducted to identify, manage, and respond to risk should be monitored on an ongoing basis. Monitoring functions are embedded in the program and assigned to any organizational level so that they can be performed in the ordinary course of running a business. Larger companies avail themselves of dedicated evaluation teams and sophisticated flowcharts and diagrams to ensure the enterprise-wide ramification of the monitoring function.<sup>83</sup>

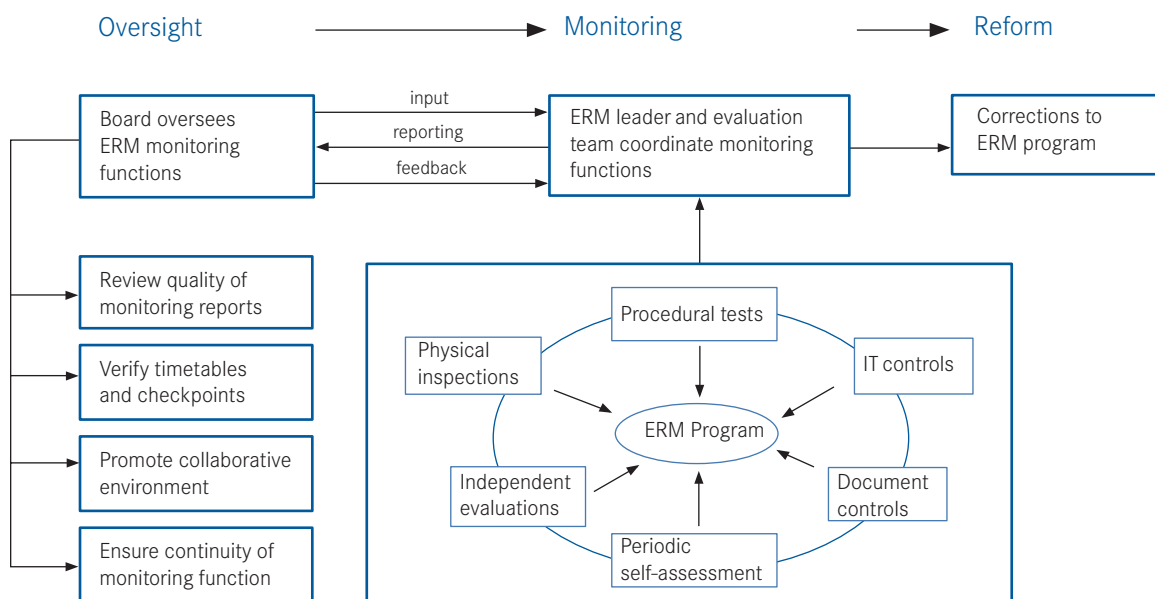
The purpose is twofold. On the one hand, by monitoring ERM on an ongoing basis, the company is able to locate, confine, and **correct the source of inaccuracies** that would distort its risk-adjusted, strategic decisions or impair its ability to pursue long-term objectives. From this point of view, monitoring channels complement upstream reporting lines. On the other hand, the monitoring function may provide feedback for future improvements to the ERM infrastructure or processes, complementing communication and educational protocols. This is the stage where senior management and board members should repeat the gap assessment conducted at the beginning of the ERM initiative, weigh the value of the work done, and determine whether there is still a business case to invest in advancing the program further.<sup>84</sup>

<sup>83</sup> For examples of how a company may document the outcomes of ERM monitoring activities, see COSO, *Enterprise Risk Management—Integrated Framework*, p. 90.

<sup>84</sup> See “Assess Gaps and Vulnerabilities in Existing Risk Management Solutions” on p. 47.

### STEP 9

In an integrated risk management environment, any activity conducted to identify, manage, and respond to risk should be monitored on an ongoing basis. Monitoring functions are embedded in the program and assigned to any organizational level so that they can be performed in the ordinary course of running a business.



“It should not be forgotten that ERM is, by nature, a work-in-progress. An important challenge for any risk management team is to keep things fresh and people engaged so that, as the company evolves, ERM also evolves,” says Smaldone of Bristol-Myers Squibb. A set of protocols to funnel feedback and implement corrections should therefore accompany each described phase of the program from event identification to assessment to risk response and reporting.

The corporate board, in particular, should review monitoring reports escalated to the attention of leading senior executives and maintain an up-to-date opinion on the quality and the efficiency of the risk management program. Directors should feel comfortable that the program contains no major deficiency or that the company is set to correct any major deficiency promptly and effectively. According to working group members, it is up to board members (or dedicated risk committee members) to verify that timetables and checkpoints ensure the continuity of the monitoring functions. Also, directors may require management to include, in their risk management performance reports, an analysis of the company’s ERM capabilities and degree of integration vis-à-vis its peers or best-in-class performers.

### Assessing performance at Capital One and MetLife

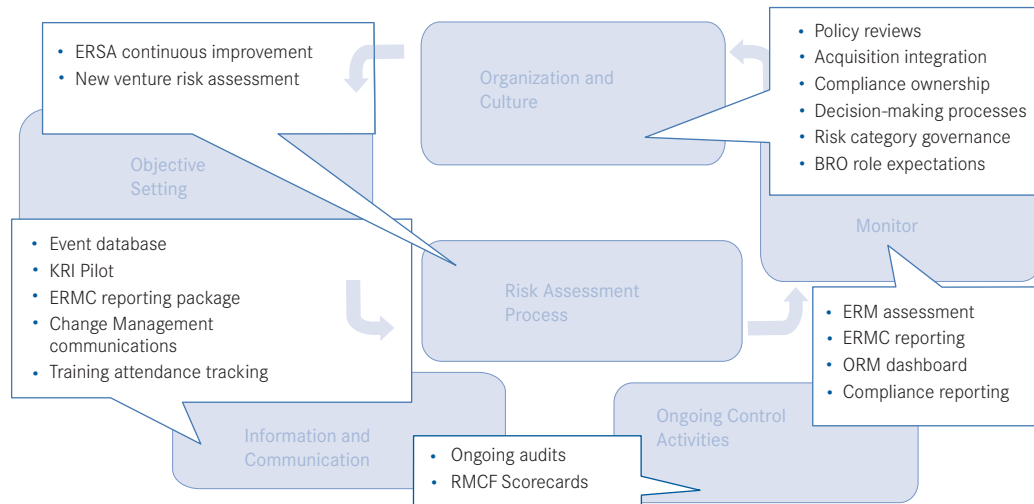
At Capital One, line managers perform ongoing monitoring functions in order to have a regular snapshot of business unit performance in the pursuit of a risk-adjusted strategy, the accuracy of risk assessments, and the conformity of risk responses adopted at the business-unit level to the entity-level risk appetite and response strategy. Ongoing control activities are composed of physical inspection of facilities, procedural tests, IT controls, and document controls (such as the review of written policies, standards, and guidelines). The internal audit office, based on its knowledge of the business and its independence, is responsible for testing and validating controls and monitoring procedures established as part of the ERM program.

In addition to its continuing verification process, Capital One has developed protocols for a periodic self-assessment by business unit managers and independent evaluations. Independent evaluations, in particular, may be prompted by exceptional circumstances or by specific incidents. For example, the failure to timely and adequately respond to a major risk event may suggest that a business unit leader has not fully understood risk tolerance levels assigned to that manager’s area of responsibility. If the incident that prompted an ad hoc evaluation had a significant impact on operations or strategy (i.e., the recall of a defective product with which the company intended to penetrate a new market, and the consequential damage caused to the company’s image), the special evaluation may be assigned to the leadership of an independent director with ERM experience or an external expert engaged by the board. In other situations, independent evaluations are conducted under the direction of a senior manager and the board is informed about their outcomes.

In 2005, after completing a first implementation of its comprehensive risk management program, Capital One’s ERM activities were directed at the continuous improvement of key components in the framework (Exhibit 19 on page 82).

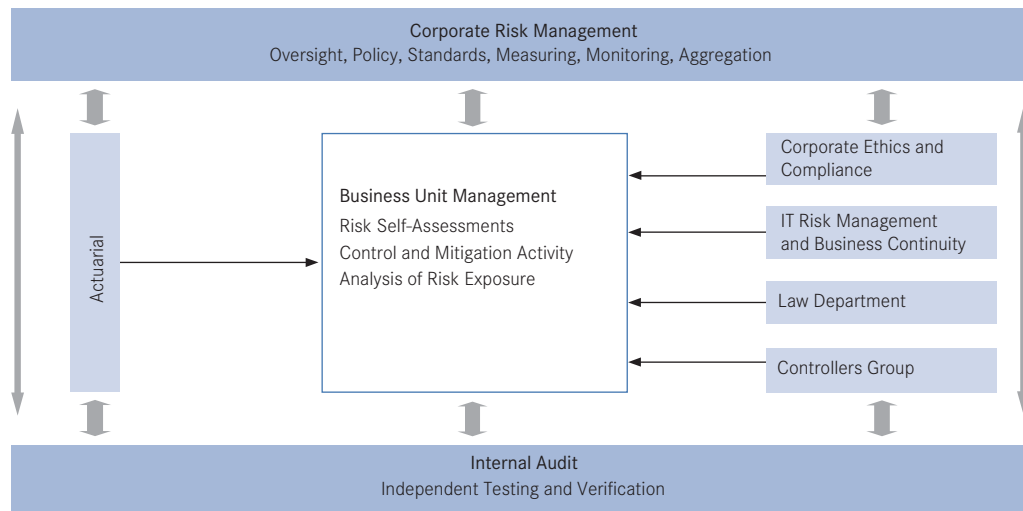
As part of the MetLife case study, the working group discussed the need for an ERM monitoring process to draw resources from most functional management offices. Corporate ethics and compliance, IT risk management and business continuity, the Controller’s department, the law department, actuaries, and internal auditors all contribute to MetLife’s overall control environment and ensure that ERM is built into the fabric of the organization (see Exhibit 20 on page 82).

Exhibit 19

**Capital One: Improving ERM**

Source: Scott Davenport, Capital One Financial Corporation, "Incorporating ERM Successfully," Presentation to The Conference Board Working Group on ERM, New York, January 10, 2006.

Exhibit 20

**MetLife: Overall Control Environment**

Source: Robin F. Lenna, MetLife, Inc., "Risk Management at MetLife: A Case Study," Presentation to The Conference Board Working Group on ERM, New York, January, 10, 2006.

# Enhancing Public Disclosure Through ERM

As an enterprise-wide infrastructure meant to embed risk analysis in the corporate strategy decision-making process, ERM is, according to Moody's Hervé Geny, a "knowledge management effort."<sup>85</sup> Through ERM, the business learns from its own organization and uses such internal knowledge to advance the pursuit of long-term goals. As a knowledge management tool, a well-crafted ERM framework may therefore become the competitive advantage that sets the company apart from its peers.

The working group discussed the need to incorporate in the ERM framework certain procedures for communicating extrafinancial information on risk and long-term strategy to stakeholders. In fact, unpublished research presented to the working group by Rick Funston, national practice leader, governance and risk oversight at Deloitte & Touche LLP, shows that risk factor disclosures included by public companies in periodic reports filed with the SEC are often inconclusive because they:

- rely heavily on boilerplate language;
- are limited to the description of individual events;
- do not attempt an analysis of the interdependencies among risk factors (whereas 80 percent of all major value losses involve a chain of events or the simultaneous occurrence of multiple events<sup>86</sup>);

- do not distinguish between rewarded and unrewarded risks (i.e., risks for which a company may either receive a premium or be punished); and
- fail to elaborate on and quantify the link between risk occurrence, strategic objectives, and enterprise value.<sup>87</sup>

Because of these limitations, public disclosure on risk contributes little knowledge to the investment process and is often overlooked by financial analysts. For this reason, a company that is implementing ERM should not miss the opportunity to enhance corporate communications on risk to the market. If the ERM framework does not improve risk disclosure procedures, the stock market will not be able to appreciate the value of what the company is doing with respect to risk management and reward it by factoring such value into the stock price. "Large investors, in particular, are suited to receive and process qualitative information on risk management, as they are often already engaged in a strategic dialogue with their portfolio companies," says Scott Davenport of Capital One. "As for the street, it increasingly asks questions on ERM, although, at this initial stage, financial analysts tend to be interested in knowing what companies are doing to protect themselves from the downside of risk. The contribution that ERM can provide to identifying and managing strategic opportunities may not yet be fully perceived."

<sup>85</sup> From remarks during a presentation to The Conference Board Working Group on ERM, January 10, 2006.

<sup>86</sup> See Mark Layton and Rick Funston, "Disarming the Value Killers: A Risk Management Study," Deloitte Research, 2005, available at [www.deloitte.com](http://www.deloitte.com).

<sup>87</sup> Rick Funston, Deloitte & Touche LLP, "Preliminary Analysis of Publicly Reported Risks," Presentation to The Conference Board Working Group on ERM, New York, November 2, 2005. The project analyzed annual reports (10-Ks, 10-Qs, and 20-F) of 266 public companies (144 of which belong to the S&P500 index). A representative sample of four or five companies was selected for each of the 51 industry segments examined.

Funston also presented a number of examples of risk factors disclosed in public company periodic reports:

**Economic conditions/trends** These include the impact of unanticipated changes in economic conditions on a company's businesses. The risk is that a company may not prepare for, identify early warning signals of, and/or fail to react quickly enough to changing economic conditions including, but not limited to, recessionary trends, inflation, job security and unemployment, financial soundness, and supplier and consumer confidence.

**Adverse legal/regulatory/environmental changes** Risks related to adverse changes in laws and regulations—including deregulation/re-regulation and those risks that threaten the company's capacity to consummate important transactions, enforce contractual agreements, or implement specific strategies and activities—in any of the jurisdictions that a company operates that may negatively impact the company's ability to do business. This risk does not include adverse court decisions or non-compliance with existing regulations.

**Competitors and competitive actions** Risks related to actions of competitors or new entrants to the market that may impair a company's competitive advantage or even threaten its ability to survive, including gradual or one-of-a-kind competitors.

**Business interruption (includes product supply interruption and natural disasters/severe weather)** Risks related to events that include natural disasters or severe weather or product supply interruption, whose outcome could have a major negative impact on the company and its ability to maintain business operations and its commitments to its customers.

**Litigation/intellectual capital issues** One example is the improper communication or inadequate protection of information (i.e., registered patents, trade secrets, etc.). Such information may be communicated to, or not protected from, individuals or competitors outside of the organization, resulting in a reduced competitive advantage. This also includes loss or theft of competitively sensitive materials by employees.

**M&A strategy/execution/integration** Mergers, acquisitions, or divestitures that are not well timed, planned, and/or executed, resulting in the acceptance of additional unwanted risk, loss of investment, or a failure to achieve intended synergies.

**Political stability/country risk** Risks include foreign corrupt practices, nationalization of company assets, difficulties in repatriating cash, compliance with embargoes, protection of intellectual property, supply disruptions, sudden adverse changes to regulations, noncompliance with rules and regulations, lack of rule of law or governance, and safety of company personnel.

**Consumer demands/preferences** Risks related to an inability to identify and effectively respond to changes in customer and market preferences, including product and service quality, and price due to priority shift, increasing customer power, resulting in flat or declining volume.

**Ability to develop/market new products** To the extent a business may be reliant on effective product development and "go-to-market" processes, the risk is that one or many of the steps in the process are not robust enough to ensure the development, fabrication, and sale of products/services that are "fit for use." This risk category encompasses the broadest definition of meeting customer needs.

**Terrorist activities/war/civil unrest** Threat of terrorist attacks, inadequate regional security, volatile local government and social conditions.<sup>88</sup>

To enhance public disclosure on risk and strategy, companies need to review their information supply chain (that is, their set of enterprise-wide procedures meant to select relevant business information, process it, and describe it in plain English) and fully integrate it with their new ERM framework. Specifically, corporations should become familiar with the use of a number of extrafinancial measurements of performance and report on those to

<sup>88</sup> Rick Funston, Deloitte & Touche, "Preliminary Analysis of Publicly Reported Risks," Presentation to The Conference Board Working Group on ERM, New York, November 2, 2005.

its stakeholders. “There is no doubt that corporations need to move away from purely financial guidance to the market,” says Amy R. Pawlicki, director, business reporting, assurance and advisory services and eXtensible Business Reporting Language (XBRL) at the American Institute of Certified Public Accountants (AICPA). “Studies indicate that, on average, only 25 percent of a company’s market value can be attributed to accounting book value, while the remaining 75 percent consists of intangible assets and expectations of future growth.”<sup>89</sup> Therefore, current annual reports—with their excessive emphasis on financial performance measures—may lack an adequate disclosure of the major value drivers of performance, including the company’s ability to face its risks and embrace their strategic upside.<sup>90</sup>

<sup>89</sup> See, for example, John Ballow, Roland Burgman, and Michael J. Molnar, “Managing for Shareholder Value: Intangibles, Future Value, and Investment Decisions,” *Journal of Business Strategy*, Volume 25, Number 5, 2004, pp. 17-22; Baruch Lev, “Remarks on the Measurement, Valuation, and Reporting of Intangible Assets,” *Economic Policy Review* (Federal Reserve Bank of New York), September 2003, pp. 17-22; and Robert Eccles, “The Performance Measurement Manifesto,” in *Measuring Corporate Performance*, Harvard Business School Press, 1991 (reprinted in 1998).

<sup>90</sup> For a more complete discussion of how business disclosure may be enhanced, see Tonello, *Revisiting Stock Market Short-Termism*, p. 27.

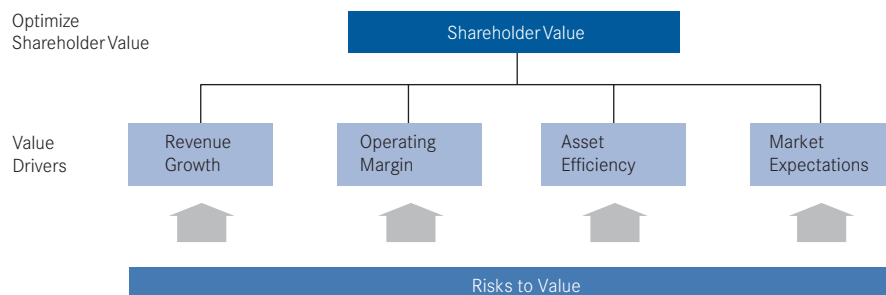
On this point, the working group members acknowledged the unprecedented change corporate reporting is undergoing. Aside from disclosure reforms passed by the SEC in the years following the enactment of the Sarbanes-Oxley Act, they recognized that certain associations and self-regulatory bodies of accounting and auditing professionals are making progress in reconsidering reporting principles and methodologies so as to provide a more complete and reliable representation of a risk-adjusted business strategy. In some cases, these projects were developed under the wing of legislatures or governments, which were receptive to the stock market need for more meaningful corporate information. In other cases, proposals are being advocated among corporate and investor leaders in the hope of garnering the largest possible support from the business community and, eventually, official ratification by public institutions.

Specifically, the Enhanced Business Reporting (EBR) Initiative was presented to the working group. The project is coordinated by a consortium of organizations (the EBR Consortium) promoted by the AICPA.

## A Value Proposition for ERM?

The following chart developed by Deloitte & Touche illustrates four major links between risk and drivers of shareholder value.

### Understanding Risks to Value



Source: Rick Funston, Deloitte & Touche, “Preliminary Analysis of Publicly Reported Risks,” Presentation to The Conference Board Working Group on ERM, New York, November 2, 2005.



## The Enhanced Business Reporting Initiative in the United States

In the United States, for many years, financial statements included in corporate reports have been accompanied by a narrative section referred to as management's discussion and analysis (MD&A). MD&A was first made mandatory by the SEC in 1974. Its scope expanded over the course of the following three decades, through a series of amendments and interpretative releases, but remained narrow. All the MD&A really intends to provide is a commentary of "financial conditions, changes in financial conditions, and results of operations."<sup>91</sup> Although a December 2003 SEC interpretative release calls for the identification and discussion of "key performance indicators, including nonfinancial performance indicators," in practice, the purpose is often defeated by the preparers' use of boilerplate language and repetitions of other parts of the annual report.<sup>92</sup> In fact, in the aftermath of the Enron scandal, the SEC conducted a thorough review of all Fortune 500 annual reports for the 2002 fiscal year. As a result, a large number of contract letters seeking amendments to the contents of reports—and especially to risk disclosures in the MD&A sections, which were found to be insufficient—were sent to filers.<sup>93</sup>

For the purpose of complementing and enhancing corporate financial statements and management commentaries (i.e., MD&A in the United States and OFR in the United Kingdom), the board of directors of the AICPA launched a proposal in 2002 to establish a collaborative effort among a large number of international stakeholders. In January 2005, the EBR Consortium was founded as a not-for-profit and independent collaboration of investors, creditors, analysts, management, directors, academics, and standard-setters charged with developing an EBR Framework. The Conference Board Governance Center joined the EBR Consortium as a strategic partner in the summer of 2005.<sup>94</sup>

On October 18, 2005, a first exposure draft of the EBR framework was released for comment from the business reporting community.<sup>95</sup> Its structure includes four new broad categories of extrafinancial disclosure: business landscape, strategy, competencies and resources, and performance (see Table 7). Each category is then articulated into a number of disclosure items. It should be noted that the framework contemplates risk management as an item of disclosure on strategy.

<sup>91</sup> See Item 303(a) of Regulation S-K under the Securities Exchange Act of 1934. It should be noted, though, that Item 101 demands a description of the business inclusive of the risk factors it is exposed to.

<sup>92</sup> SEC Release No. 33-8350; 34-48960 ("Interpretation: Commission Guidance on Management's Discussion and Analysis of Financial Condition and Results of Operations"), December 29, 2003.

<sup>93</sup> See "Summary by the Division of Corporation Finance of Significant Issues Addressed in the Review of the Periodic Reports of the Fortune 500 Companies," February 27, 2003, available at [www.sec.gov/divisions/corpfin/fortune500rep.htm](http://www.sec.gov/divisions/corpfin/fortune500rep.htm).

<sup>94</sup> In addition to the AICPA, the founding members of the EBRC are Grant Thornton LLP, Microsoft Corporation, and PricewaterhouseCoopers LLP. Other strategic partners include The Business Roundtable, National Association of Corporate Directors, and NASDAQ.

<sup>95</sup> The Enhanced Business Reporting Framework, Public Exposure Draft, October 2005. The draft can be downloaded at [www.ebr360.org](http://www.ebr360.org). Also see Robert G. Eccles and Amy R. Pawlicki, "From Financial Reporting to Comprehensive Corporate Performance Reporting," Presentation to The Conference Board Working Group on ERM, New York, November 2, 2005. The "Enhanced Business Reporting Framework" and related EBR materials are substantially based on and refer to the PricewaterhouseCoopers's Value Reporting materials and research. The copyright of PricewaterhouseCoopers's Value Reporting materials is owned by PricewaterhouseCoopers, and all rights are reserved. For information on the PricewaterhouseCoopers Value Reporting program, see [www.corporatereporting.com](http://www.corporatereporting.com).

Table 7

**Enhanced Business Reporting Framework**

<i>Level 1</i>	<i>Level 2</i>
<b>Business Landscape</b>	Overview Competition Customers Technological change Shareholder relations Capital availability Legal Political Regulatory
<b>Strategy</b>	Business model Organization Governance Risk management Environmental and social Business portfolio Resource allocation Product life cycle
<b>Competencies &amp; Resources</b>	Key processes Customer satisfaction People Innovation Supply chain Intellectual property Information and technology Financial assets Physical assets
<b>Performance</b>	Profitability Liquidity Operating

Source: *The Enhanced Business Reporting Framework, Exposure Draft*, AICPA, October 2005.

The EBR Framework was also devised to permit the use of taxonomies (such as XBRL)<sup>96</sup> for the classification of companies on the basis of their value drivers, performance measures, and qualitative information on strategy and risk. In other words, through EBR, market participants (investors, analysts, etc.) will be able to extract from public filings specific information they need in their evaluation of corporate performance.

“Enhanced business reporting can change the markets’ focus on short-term earnings projections,” says Robert Eccles, a working group member and an advisor to the EBR Consortium and former Harvard Business School professor. “The over-emphasis on quarterly earnings will decline as companies report transparently on their key drivers of value creation. The long-term rewards will be tangible: a greater investor following, lower stock-price volatility, and ultimately a more attractive cost of equity and debt.”<sup>97</sup>

<sup>96</sup> XBRL stands for eXtensible Business Reporting Language. It is an open standard (free of license fees) for the electronic communication of business and financial data being developed by an international nonprofit consortium of approximately 250 major companies, organizations, and government agencies. It is already being put to practical use in a number of countries and implementations of XBRL are growing rapidly around the world (an XBRL Voluntary Program was launched by the U.S. SEC in early 2005). In a speech held at the 12th XBRL International Conference in Tokyo on November 7, 2004, SEC Chairman Christopher Cox stated: “Interactive data promises more than simply a revolution in corporate reporting. For the SEC [the XBRL Voluntary Program] is an opportunity to assess how the use of interactive data can help us improve our internal review of information, and how it can help us make it available in more useful form to the public.” See [www.sec.gov/news/speech/spch110705cc.htm](http://www.sec.gov/news/speech/spch110705cc.htm).

<sup>97</sup> See the Enhanced Business Reporting Consortium press release of October 18, 2005 (“Enhanced Business Reporting Consortium Releases Framework to Promote Greater Transparency in Corporate Reporting”). Robert Eccles is among the most influential scholars who have been advocating the need to revise the system for the communication of enterprise value drivers. Eccles’s research on reforming corporate reporting is extensive; in addition to the work cited elsewhere in this report, see, for example: “Improving the Corporate Disclosure Process,” *Sloan Management Review*, Volume 36, Number 4, 1995, pp. 11-25 (with Sarah C. Mavrinac); *Value and Reporting in the Banking Industry*, PricewaterhouseCoopers, 1999 (with John K. Fletcher); and *Value and Reporting in the Insurance Industry*, PricewaterhouseCoopers, 1999 (with Michael P. Nelligan).

## Other Initiatives to Reform Business Reporting

The U.K.'s **Operating and Financial Review (OFR)** contemplated legally requiring directors of quoted companies to prepare a narrative top-down analysis of where the business stood in the pursuit of its objectives. In November 2005, however, the British Government scrapped the requirement from the Company Law Reform Bill then under discussion due to concerns about the imposition of unnecessary burdens on U.K. companies.\*

The **International Accounting Standards Board's (IASB)** 2005 Discussion Paper on **Management Commentary**, which concludes that the IASB should issue a standard to provide non-mandatory guidance for the disclosure of corporate information on: (a) the nature of the business; (b) its objectives and strategy; (c) its key resources, risks, and relationships; (d) its results and prospects; and (e) its performance measures and indicators.\*\*

The **European Union Accounts Modernization Directive of 2003**, under which certain public companies listed in EU stock markets are required to include in their annual reports "a balanced and comprehensive analysis of the

development and performance of the company's business and of its position, together with a description of the principal risks and uncertainties that it faces.... To the extent necessary for an understanding of the company's development, performance, or position, the analysis shall include both financial and, where appropriate, nonfinancial key performance indicators relevant to the particular business, including information relating to environmental and employee matters."\*\*\*

Although the concept of MD&A outlined in **The International Organization of Securities Commission's (IOSCO) 2003 General Principles Regarding Disclosure of Management's Discussion and Analysis of Financial Condition and Results of Operations** does not depart from a commentary of financial results, IOSCO indicates that "care should be taken to avoid the use of boilerplate or stock language that appears to be in technical compliance with disclosure requirements, but that nonetheless fails to provide investors with appropriate information they need to make valuation and investment decisions."\*\*\*\*

\* See Janice Lingwood, PricewaterhouseCoopers, "OFR and IASB Management Commentary," Presentation to The Conference Board Working Group on ERM, New York, November 2, 2005.

\*\* *Management Commentary*, International Accounting Standards Board, October 2005, Section 4.100, p. 33.

\*\*\* Article 46(1) of Directive 2003/51/EC of the European Parliament and of the Council of 18 June 2003 amending Directives 78/660/EEC, 83/349/EEC, 86/635/EEC, and 91/674/EEC on the annual and consolidated accounts of certain types of companies, banks, and other financial institutions and insurance undertakings, OJ L 178, 17/07/2003, pp. 16-22.

\*\*\*\* *General Principles Regarding Disclosure of Management's Discussion and Analysis of Financial Condition and Result of Operations*, IOSCO, 2003.

The Conference Board working group discussed the governance role of the corporate board in the oversight of ERM disclosure procedures. The following aspects were underscored:

- The need for a high-level discussion on how to set an **ERM competitive advantage** and convey to securities analysts and investors the value inherent in the company's ERM effort.
- The need to ensure that **ERM is fully integrated with existing corporate disclosure procedures** so that any material, nonconfidential information on business risk is captured and adequately communicated to the market.
- The need to be satisfied with the **transparency of the disclosure process**. Specifically, the board should verify that any individual involved in the risk management program is in a position to raise concerns regarding the accuracy and completeness of disclosed information on risk without fear of retaliation or retribution.
- The need to ensure that authorization and other **verification protocols** are in place so that the disclosure of qualitative, extrafinancial performance measures is not manipulated by those managers who participate in the information-supply chain.
- The possibility of promoting a **voluntary trial program** for the dissemination of enhanced disclosure on the long-term, risk-adjusted business strategy. The program could be organized under the high-level supervision of the corporate board and involve a selected group of financial analysts and institutional investors. The purpose of the program would be to assess—with direct help from other market participants—the relevance of information regarding risk and strategy on the investment decision-making process.

## Recommendations on Risk Disclosure by The Conference Board Corporate/Investor Summit Delegates

The use of ERM as a tool to enhance business disclosure was also discussed at the Corporate/Investor Summits on stock market short-termism held by The Conference Board Governance Center in London (July 2005) and Washington, D.C. (March 2006). Delegates to the summits included distinguished representatives from the corporate world, the institutional investment community, the financial service industry, and academia.

According to summit delegates, “the widespread adoption of an Enterprise Risk Management framework should be encouraged as an effective process to assess and respond to strategic and operating risks, not only to bring clarity to the long-term strategic direction a business should take, but also to clearly communicate such long-term strategy to the market.” The following are the recommendations made by summit delegates to meet this goal:\*

- Further studies should be undertaken regarding the **deployment of intangible corporate assets** such as a set of rigorous corporate governance practices and an integrated risk management infrastructure. Research should be diversified by type of industry and geographical region, so as to develop a set of sector-specific financial and extrafinancial performance metrics to assess the ability of a company to appreciate and respond to financial and business risks, while embracing the strategic opportunities that may derive from business risks. Such metrics could then be embraced and disseminated by business associations, encouraging their best practices implementation by the leading companies in the industry or fostering the development of sector-based voluntary frameworks for extrafinancial reporting.
- As risk-adjusted, qualitative performance metrics are better identified, a related body of research on the **negotiation of compensation schemes** tied to the quality of risk management may be furthered. For this purpose, The Conference Board Governance Center undertook in the summer of 2006 a case-study based research project to investigate what extrafinancial measures are being deployed and how they are articulated, verified, and communicated to the market.
- Further research on extrafinancial measures of performance should be based on **voluntary trial programs** where, in addition to filing their regular annual reports, participating companies provide financial analysts and large investors with a more comprehensive set of information on their value drivers (including the quality of risk assessment and response). Comparative information on how the response from investors and analysts varies according to the report they read would be helpful to assess the viability of the proposed “best practice” framework.
- Proposed disclosure frameworks to enhance corporate transparency on intangible assets (including the robustness of ERM) and extrafinancial measures of performance should be supported by **empirical research on their application**. As noted in this report, a number of enhanced disclosure frameworks are being developed. Although such proposals come from public or not-for-profit institutions, the competition among sponsoring organizations may generate confusion and undermine their credibility. Moreover, in the currently overregulated securities market, any attempt at expanding reporting requirements may encounter the resistance of business lobbying groups, which fiercely oppose imposing any extra cost of compliance. A reliable set of data on the market appreciation for the practical use of a certain framework would therefore facilitate the natural selection of one “best practice” model and encourage its widespread adoption.

\* See also Matteo Tonello, *Revisiting Stock Market Short-Termism*, R-1386-06-RR, 2006, p. 43.

# Conclusion

Research conducted by The Conference Board Working Group on ERM revealed the need for a common base of practical guidance on how corporate boards and senior executives should address the corporate governance implications of integrating risk management at their companies. Although there is no “one-size-fits-all” enterprise risk management process, working group members identified a number of emerging practices regarding the establishment of an ERM infrastructure, the assignment of responsibilities, and the design of a working program.

While many organizations have been engaging in some aspects of ERM, only a few have developed a full-fledged program to incorporate a comprehensive risk analysis in their top-level strategy-setting activities. The inquiries conducted by the working group revealed the need to pursue further research and to develop a broad consensus regarding practices under development in three major areas of ERM implementation:

- The choice of compensation policies and performance metrics to promote and track the pursuit of a risk-adjusted corporate strategy.
- The integration of ERM with existing operational systems (i.e., IT, accounting/budgeting/planning, internal control, regulatory compliance, etc.).
- The enhancement of public disclosure on long-term, risk-adjusted strategic goals.

Through its research projects on risk governance, The Conference Board Governance Center continues to address the multi-faceted issue of stock market short-termism according to the recommendations made by delegates to the Corporate/Investor Summit held in London in July 2005. In the view of summit delegates, “widespread adoption of an Enterprise Risk Management framework should be encouraged as an effective process to assess and respond to strategic and operating risk, not only to bring clarity to the long-term strategic direction a business should take, but also to clearly communicate such long-term strategy to the market.”<sup>98</sup>

---

<sup>98</sup> See Tonello, *Revisiting Stock Market Short-Termism*, p. 43.



# The ERM Road Map

## Emerging Governance Practices

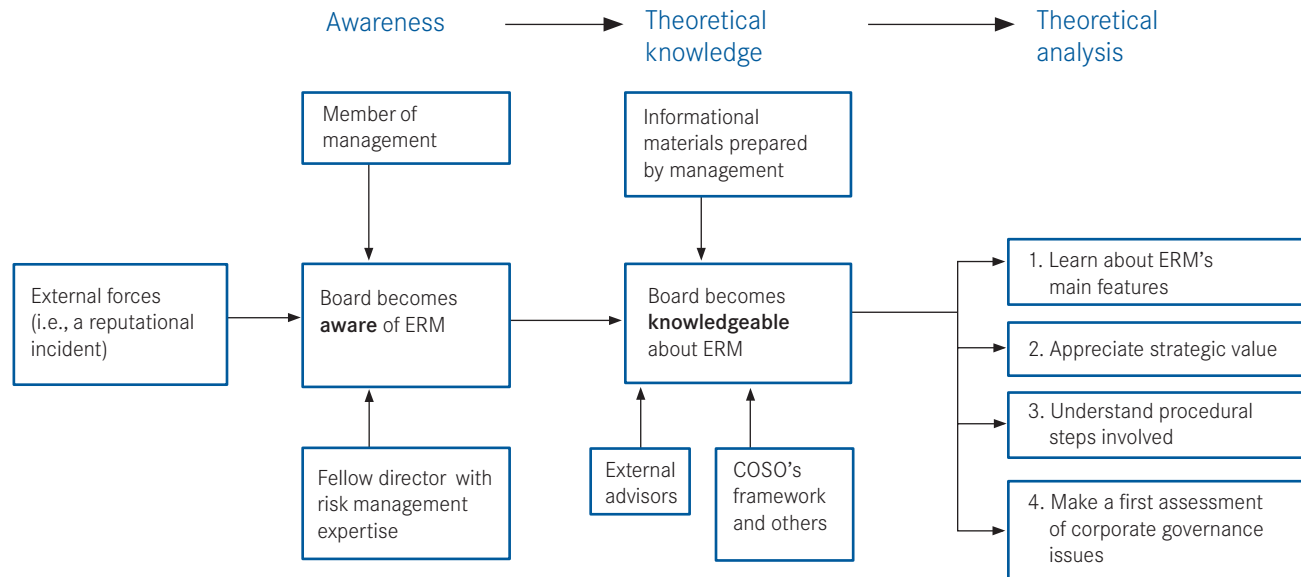
This “road map” to enterprise risk management implementation was developed from the case studies discussed by The Conference Board Working Group on Enterprise Risk Management. It is intended as an easy-reference analytical tool for use by corporate boards to fulfill their oversight duties and understand the range of potential corporate governance issues related to managing risk in an integrated, top-down, and strategic manner.





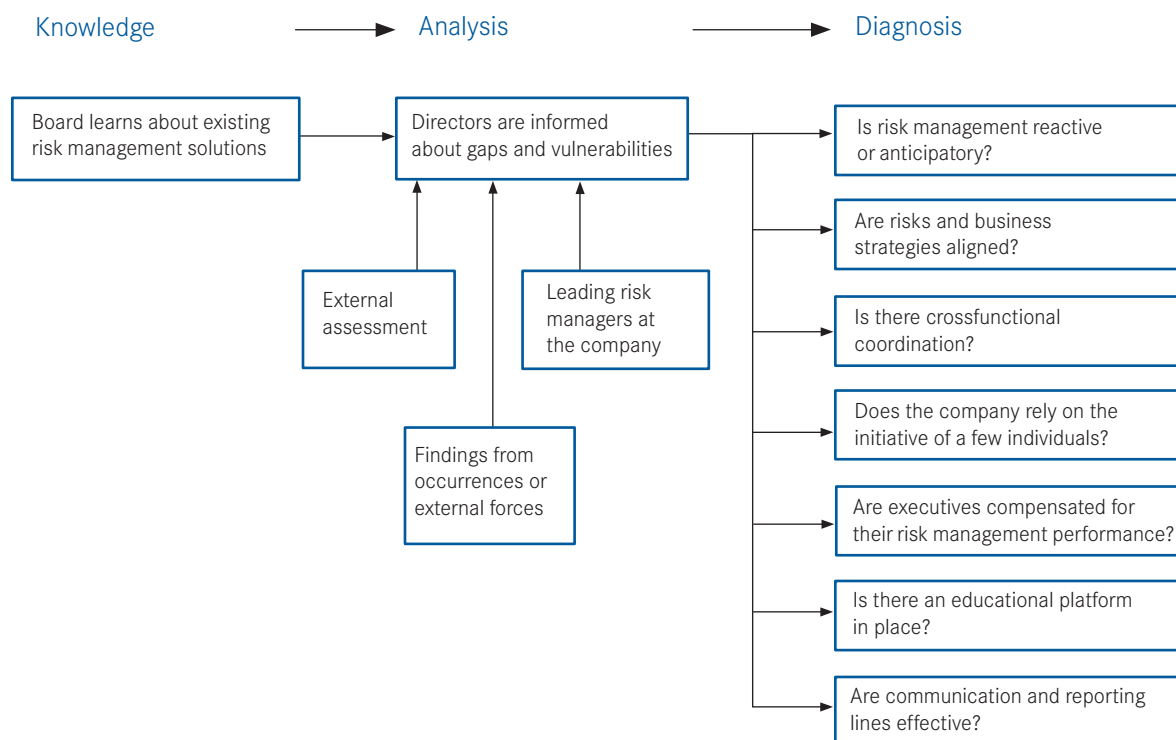
## STEP 1 Appreciate the Importance of Enterprise Risk Management

The first fundamental step in jump-starting ERM is to bring awareness of its existence, features, and potential benefits to the board. Members of the board of directors become knowledgeable about and come to appreciate the value ERM can add to their strategic and operational decision-making process. They also make a first assessment of corporate governance issues that may arise during program implementation.



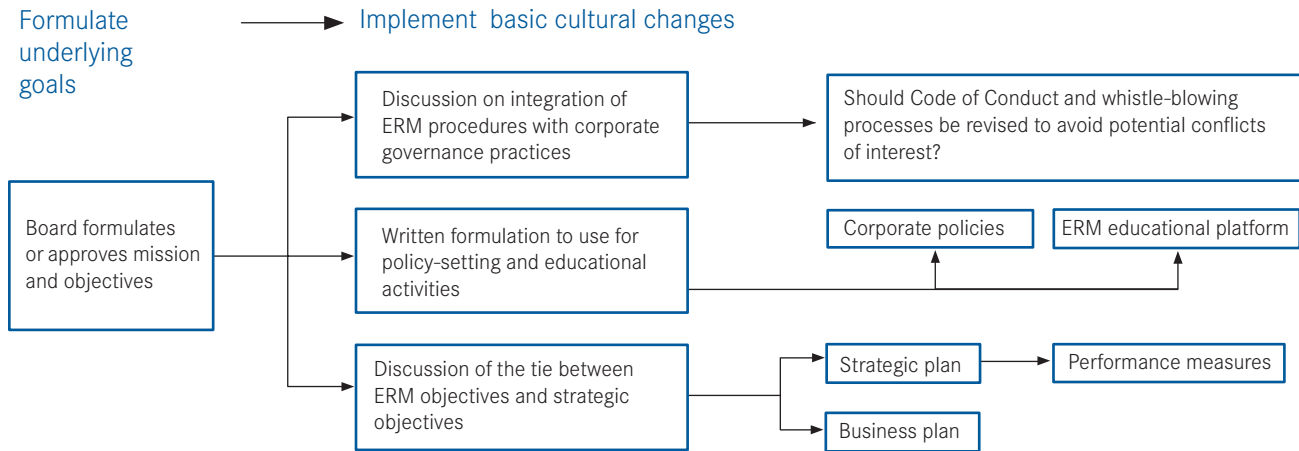
## STEP 2 Assess Gaps and Vulnerabilities in Existing Risk Management Solutions

The business case for implementing ERM should rest on a detailed analysis of the limitations inherent in current risk management solutions. A company may perform well with respect to managing certain repetitive occurrences, but lack a sustainable process to expand its view of business risk and predispose an enterprise-wide response strategy.



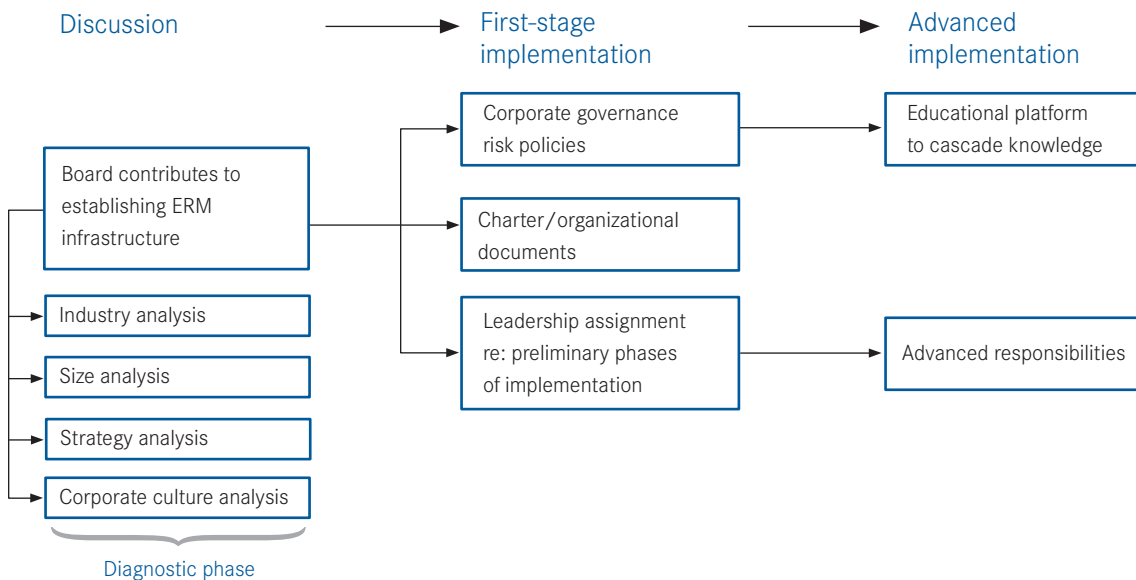
### STEP 3 Set Underlying Mission and Program Objectives

At this point, the business case for ERM should be formulated as a concise and effective mission statement and articulated in the main objectives for the program. The ERM program's objectives should be tied to the firm's strategic objectives. While the mission statement summarizes the vision shared by board members and senior executives, program objectives should consist of a list of actionable goals to communicate to the whole organization.



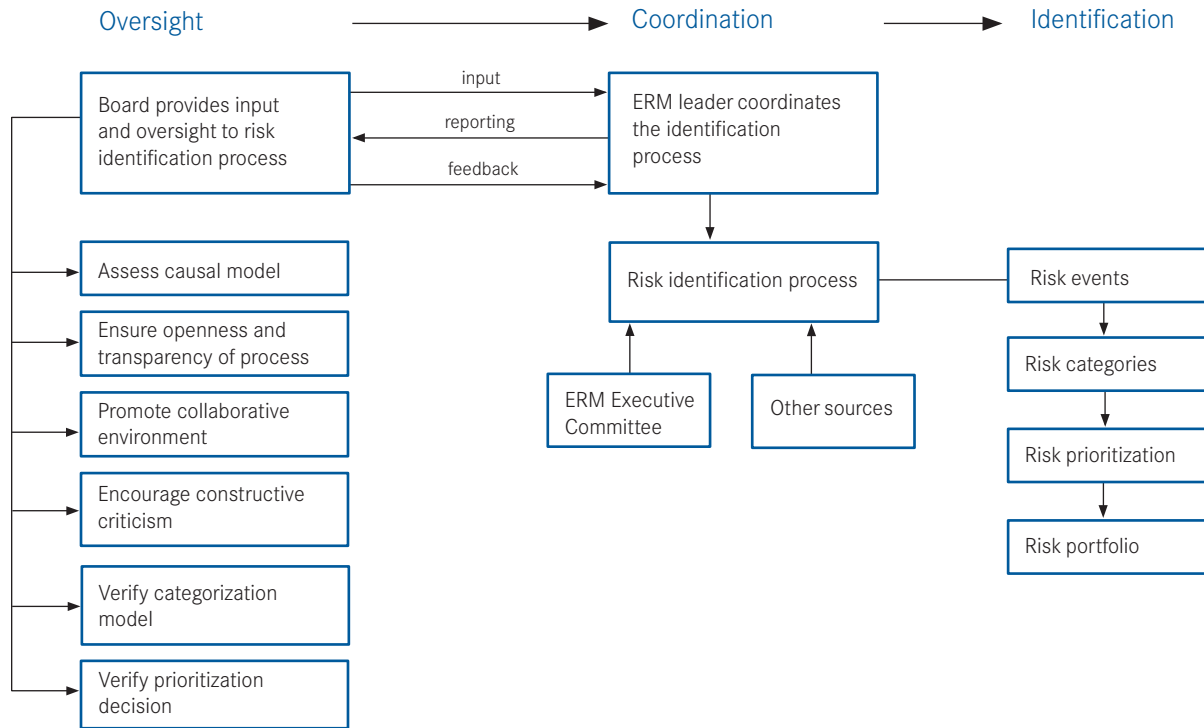
### STEP 4 Establish the ERM Infrastructure and Assign Leadership

Risk governance policies, executive leadership, delegation of authorities, and a system of accountability should be part of the top-level discussion on the establishment of an ERM infrastructure.



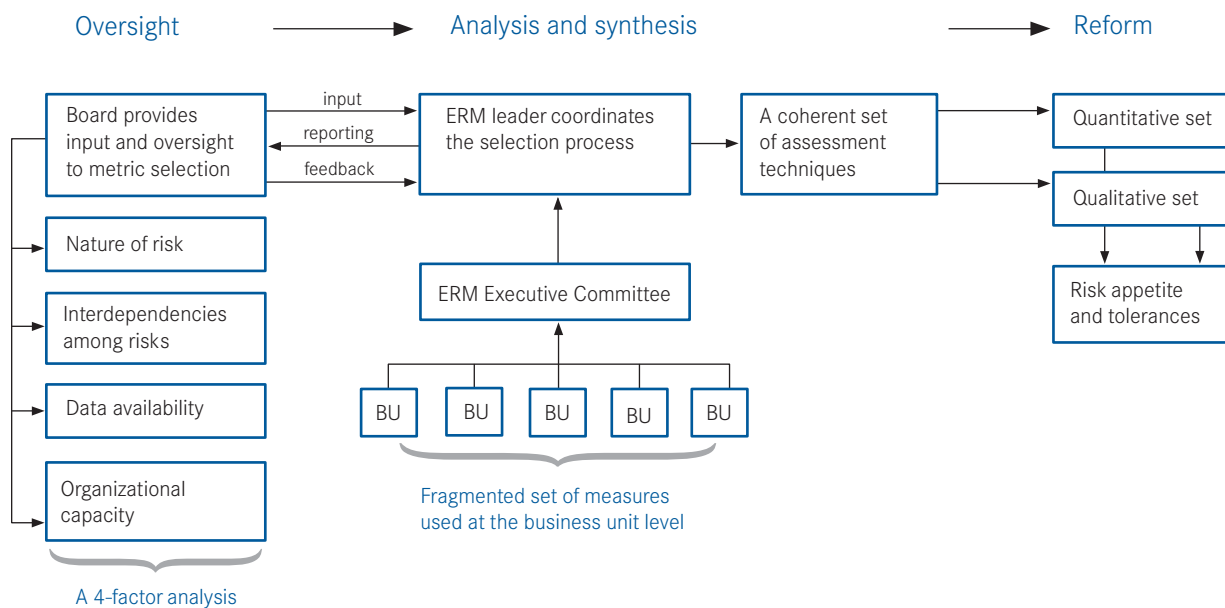
## STEP 5 Compile a Risk Inventory

From a corporate governance standpoint, the role of the board of directors in the compilation of a risk inventory cannot be overstated. In this phase, board members not only contribute their knowledge and expertise, but also oversee the process adopted by senior management to identify and prioritize risks.



## STEP 6 Select Assessment Techniques and Define Risk Appetite and Tolerance

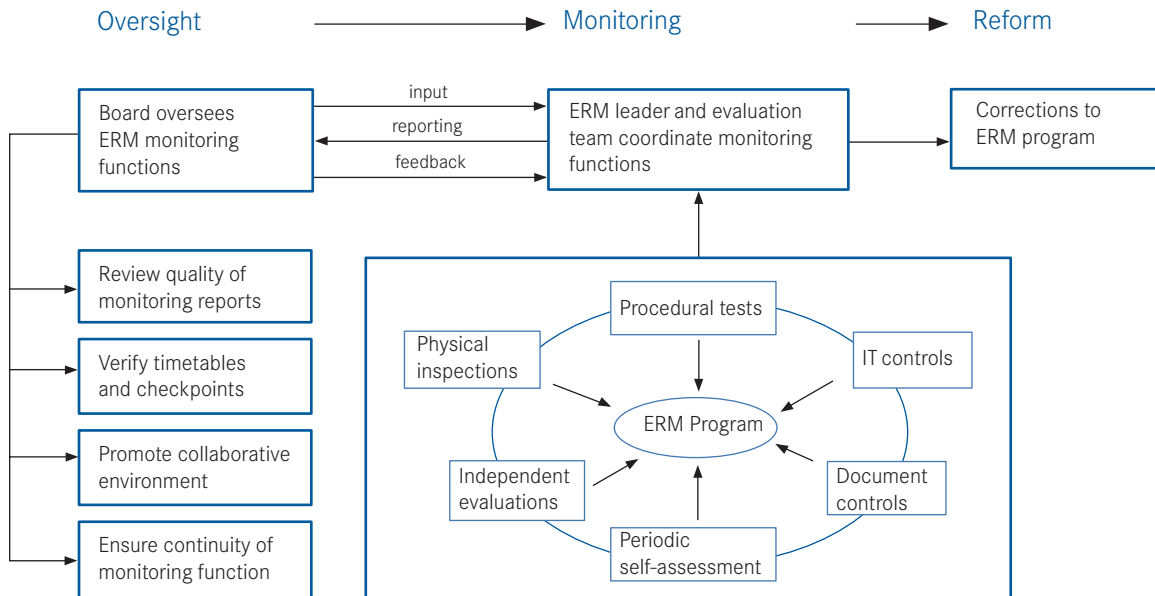
Once business risks are identified and grouped into a reasonably limited number of categories, senior management should agree upon a set of measures and techniques to assess the relevance of each item in the inventory. Functional managers, business unit leaders, and other risk owners will then be trained to employ those measures and techniques as part of the ERM process.





## STEP 9 Monitor ERM Implementation and Execution

In an integrated risk management environment, any activity conducted to identify, manage, and respond to risk should be monitored on an ongoing basis. Monitoring functions are embedded in the program and assigned to any organizational level so that they can be performed in the ordinary course of running a business.



## Working Group Members and Speakers

**Chester Paul Beach, Jr.**  
Associate General Counsel  
United Technologies  
Corporation<sup>†</sup>

**Mark S. Beasley**  
Professor, Department of  
Accounting  
Director, Enterprise Risk  
Management Initiative  
College of Management  
North Carolina State  
University

**Caryn Bocchino**  
Senior Manager  
KPMG's Audit Committee  
Institute<sup>†</sup>

**John T. Bostelman\***  
Partner  
Sullivan and Cromwell LLP

**Carolyn K. Brancato**  
Director  
Governance Center  
The Conference Board, Inc.

**Thomas Brier**  
Deputy Director for Corporate  
Governance  
Pennsylvania State  
Employees' Retirement  
System<sup>†</sup>

**Laura L. Brooks**  
Vice President,  
Risk Management, and  
Chief Risk Officer  
Public Service Enterprise  
Group<sup>†</sup>

**Carlton J. Charles\***  
Head of Enterprise  
Risk Management  
International Paper Company

**Karen Clapsaddle**  
Director, Compliance Programs  
and Global Ethics  
Lockheed Martin Corporation<sup>†</sup>

**George S. Dallas**  
Managing Director and  
Global Practice Leader,  
Governance Services  
Standard & Poor's

**Scott Davenport\***  
Vice President, Enterprise Risk  
Management  
Capital One Financial  
Corporation

**Nancy A. DeRiso**  
Vice President and  
Director of Internal Audit  
Selective Insurance Group<sup>†</sup>

**Robert G. Eccles\***  
President  
Advisory Capital Partners, Inc.

**Miles Everson\***  
Partner  
PricewaterhouseCoopers LLP<sup>†</sup>

**Craig Faris\***  
Director  
Mercer Oliver Wyman

**John M. Farrell\***  
Partner  
KPMG's Audit Committee  
Institute<sup>†</sup>

**Donna Fletcher**  
Associate Professor of Finance,  
Director of Risk Management  
Program  
Hughey Center for Financial  
Services  
Bentley College<sup>†</sup>

**William Foote**  
Enterprise Risk Services  
Director  
Deloitte & Touche LLP<sup>†</sup>

**Rick Funston\***  
National Practice Leader,  
Governance and Risk Oversight  
Deloitte & Touche LLP<sup>†</sup>

**Hervé Geny\***  
Senior Vice President  
Moody's Corporation

**Sylvia Gentzsch**  
Manager  
Governance and Risk  
Oversight  
Deloitte & Touche LLP<sup>†</sup>

**Thomas Graham**  
Senior Staff, Strategy and  
Planning Group, Corporate  
Internal Audit  
Lockheed Martin Corporation<sup>†</sup>

**Todd Greenwald**  
Head of Operational Risk  
TIAA-CREF<sup>†</sup>

**Kent Harvey**  
Senior Vice President, CFO and  
Treasurer  
PG&E Corporation<sup>†</sup>

**Eric Henry**  
Executive Director  
Pennsylvania State  
Employees' Retirement  
System<sup>†</sup>

**Ellen Hexter\***  
Senior Advisor on Integrated  
Risk Management  
The Conference Board, Inc.

**Gary L. Lavey**  
Vice President, Global Risk  
Management  
Cinergy Corporation<sup>†</sup>

**Robin F. Lenna\***  
Senior Vice President and Chief  
Risk Officer  
MetLife, Inc.

**Janice Lingwood\***  
Director, UK Value Reporting  
PricewaterhouseCoopers LLP<sup>†</sup>

**Steven Oster**  
Director, Enterprise Risk  
Strategy  
Public Service Enterprise  
Group<sup>†</sup>

**Kenneth Pavlick**  
Internal Audit Manager  
Selective Insurance Group<sup>†</sup>

**Amy Pawlicki\***  
Director - Business Reporting,  
Assurance & Advisory Services  
and XBRL  
American Institute of CPAs  
Inc.

**John Phelps**  
Director of Risk Management  
BlueCross BlueShield of  
Florida

**Michael Privitera**  
Vice President, Public Affairs  
Standard & Poor's<sup>†</sup>

**Mary Jane Raymond\***  
Chief Risk Officer  
Dun & Bradstreet Corporation

**Scott A. Reed**  
Partner  
KPMG's Audit Committee  
Institute<sup>†</sup>

**Prodyot Samanta\***  
Director, Enterprise Risk  
Management  
Standard & Poor's<sup>†</sup>

**Michele N. Schumacher**  
Vice President, Corporate  
Secretary, and Corporate  
Governance Officer  
Selective Insurance Group<sup>†</sup>

**Laurie F. Smaldone\***  
Vice President, Strategy and  
Issues Management  
Bristol-Myers Squibb Company

**Matteo Tonello**  
Senior Research Associate  
Governance Center  
The Conference Board, Inc.

**Janice Wilkins**  
Vice President and  
Director of Internal Audit  
Intel Corporation<sup>†</sup>

**Charles Windeknecht\***  
Director, Internal Audit  
Moody's Corporation

<sup>†</sup> Governance Center Advisory  
Board member

<sup>‡</sup> Governance Center member

\* Speaker

**Navigating Risk: The Business Case for Security**

Research Report 1395, 2006

**The Role of U.S. Corporate Boards in Enterprise Risk Management**

Research Report 1390, 2006

**Enterprise Risk Management Systems: Beyond the Balanced Scorecard**

Special Report 9, 2005

**From Risk Management to Risk Strategy: Mid-Markets**

Research Report 1368, 2005

**From Risk Management to Risk Strategy**

Research Report 1363, 2005

**Keep It Simple: Getting Your Arms Around Enterprise Risk Management**

Executive Action 165, 2005

**The Conference Board Governance Center**

The Governance Center is composed of a distinguished group of senior executives from leading world-class companies and influential institutional investors. Membership provides:

- Valuable networking: Access a global organization of major companies and institutional investors who share common interests and issues.
- Relevant knowledge: Share perspectives with prominent senior executives from global companies in meetings, workshops, and symposia.
- High visibility: Be a key part of domestic and international events and research projects through sponsorship.
- Team approach: Executives within a company can participate together, encouraging teamwork and leveraging the individual experience.
- Cutting-edge research: Benefit from the Governance Center's research on trends and best practices, both in the United States and internationally.

**The Conference Board Directors' Institute**

The premier provider of governance education for directors, the Directors' Institute offers both roundtable forums and customized in-house forums. The Directors' Institute brings together current and former directors, chairmen, and CEOs to share their experiences and wisdom with company directors in a completely non-academic, hands-on format.

- Only foremost directors and practitioners – not academics – serve as faculty.
- Topics cover practical “real-world” and “red-flag” issues.
- Limited session size and restricted attendance to sitting directors provides high-level peer dialogue.
- One intensive program provides directors with a time-efficient method of getting up to speed with the latest best practices.
- The Conference Board Directors' Institute programs are accredited by ISS as a “preferred Boardroom Education Program.”

Publishing Director **Chuck Mitchell**

Author **Matteo Tonello, LL.M., Ph. D.**

Editor **Timothy Dennison**

Design **Peter Drubin**

Production **Pam Seenaraine**

**The Conference Board, Inc.**

845 Third Avenue  
New York, NY 10022-6600  
United States  
Tel +1 212 759 0900  
Fax +1 212 980 7014  
[www.conference-board.org](http://www.conference-board.org)

**The Conference Board Europe**

Chaussée de La Hulpe 130, box 11  
B-1000 Brussels  
Belgium  
Tel +32 2 675 5405  
Fax +32 2 675 0395  
[www.conference-board.org/europe.htm](http://www.conference-board.org/europe.htm)

**The Conference Board Asia-Pacific**

22/F, Shun Ho Tower  
24-30 Ice House Street, Central  
Hong Kong, SAR  
Tel +852 2804 1000  
Fax +852 2869 1403  
[www.conference-board.org/ap.htm](http://www.conference-board.org/ap.htm)

**The Conference Board of Canada**

255 Smyth Road  
Ottawa, Ontario K1H 8M7  
Canada  
Tel +1 613 526 3280  
Fax +1 613 526 4857  
[www.conferenceboard.ca](http://www.conferenceboard.ca)