Risk Practice

McKINSEY WORKING PAPERS ON RISK

Making risk management a value-adding function in the boardroom

Number 2
September 2008

André Brodeur and
Gunnar Pritsch

McKinsey&Company

Making risk management a value-adding function in the boardroom

Contents

McKinsey Working Papers on Risk is a new series presenting McKinsey's best current thinking on risk and risk management. The papers represent a broad range of views, both sector-specific and cross-cutting, and are intended to encourage discussion internally and externally. Working papers may be republished through other internal or external channels. Please address correspondence to the managing editor, Andrew Freeman, andrew_freeman@mckinsey.com

Introduction

During the past decade, unforeseen risk combined with either poor or good risk management often had more impact on corporate performance than superior strategy or outstanding execution. Some companies proved unlucky. Continental Airlines, for example, had completed a remarkable turnaround and was enjoying considerable profitability when surging fuel costs drove it back into the red. Southwest Airlines, in contrast, having hedged its fuel prices all the way to 2009, was able to remain profitable in 2005.[1] And still other companies hit the jackpot. Lakshmi Mittal is now one of the world's richest men, mainly because Mittal Steel had rolled up marginal assets just before a dramatic increase in steel prices.

Taking risks is a part of being in business. Although the outcome of key uncertainties is often dictated by luck, the impact of these outcomes is not. Good risk management can help mitigate the impact of negative outcomes and help companies take advantage of positive ones.

Today's board directors are well aware of the importance of managing risks explicitly, especially as the meanings of "good faith" and "reasonable care" are continuing to evolve. It is thus reassuring that boards appear increasingly confident about their abilities to handle risk (Exhibit 1). It is the rare director who admits to not knowing what's going on with respect to risk – an admission not uncommon just 5 years ago. In fact, a recent survey indicated that only 1 percent of directors report not having a process to identify, safeguard, and plan for key risks – compared in 2002 to 19 percent.[2]

Clearly, U.S. boards have come a long way in improving their approaches to enterprise risk management (ERM). However, the concept of ERM as an offensive discipline – a function that can maximize enterprise value when fully leveraged – is only starting to emerge. At many companies, much remains to be done before ERM can deliver its full value-adding potential.

Based on McKinsey & Company's research and experience in enterprise risk management and governance, we believe that many boards are operating with a false sense of security. For these board members, ERM is still primarily about complying with new regulatory standards, many of which they consider overly bureaucratic (e.g., Sarbanes-Oxley).

This working paper first examines the ERM landscape: current shortfalls, potential benefits, and approaches. To the growing body of common wisdom about ERM, it then adds eight recommendations designed to help boards understand, monitor, and manage risk more effectively.

1 For example, analysts estimate that in 2005 Southwest had 85 percent of its fuel price hedged at $26 a barrel; at that time, Continental's cost per barrel had risen to well above $50.

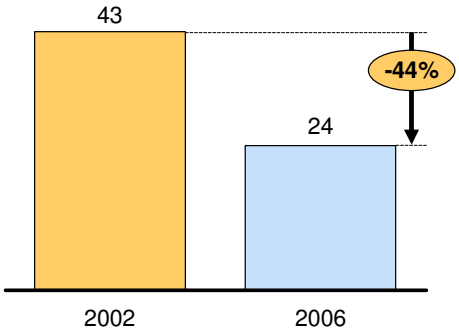
2 This white paper summarizes viewpoints from McKinsey & Company's enterprise risk management and governance work with leading companies, and from a joint research project with The Conference Board: *The Role of the U.S. Corporate Board of Directors in Enterprise Risk Management* (The Conference Board, New York, 2006). Cited here are responses to McKinsey's survey for *Director Magazine* (2002), as well as interviews with 30 board members and a written survey of directors (127 respondents) conducted by McKinsey in conjunction with The Conference Board and KPMG's Audit Committee Institute from October 2005 to February 2006.

EXHIBIT 1

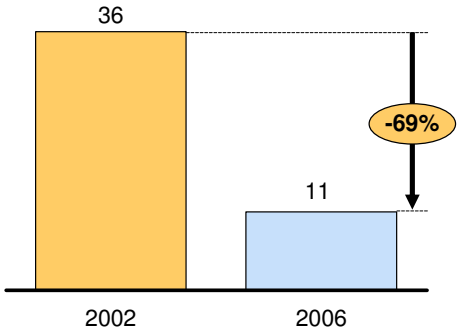
Directors believe that their handling of risk has improved over the past 4 years

Survey findings – February 2006
Percent of respondents

"Our process to identify, safeguard, and plan for key risks is either nonexistent or ineffective"



"We have only a partial understanding of the major risks the company is facing"



At the outset, a false sense of security

While the increased comfort directors have expressed in dealing with risk is a welcome development, the persistent gaps in risk management capabilities and the changing legal and regulatory environments suggest that things may not be as buttoned-down as they appear.

Persistent gaps in risk management capabilities

Perhaps most important, few directors – despite their self-declared comfort with risk – pursue a disciplined approach to ERM. According to the survey, most have yet to master some of the basics of risk management. For example:

- Only 17 percent of U.S. directors report that their boards have established a risk inventory. Furthermore, only 48 percent report that their boards rank risks or can gain access to structured risk information like heat maps – typical indications of a robust process for evaluating risk. Most companies that do rank risks, do so annually.
- Nearly 60 percent of directors acknowledge that they lack a fair understanding of how the business's different parts interact in the overall company's risk portfolio.

- Close to 30 percent of directors interviewed express concerns about their fellow directors' understanding of key risks, though directors in the bank and insurance sectors report less variation in risk knowledge than their peers in nonfinancial industries.

Directors we talked to at nonfinancial firms report significant variations in practices across industries and believe significant opportunities still exist to learn from best practices. Nearly 75 percent of directors who sit on multiple boards report significant variations in ERM capabilities across firms and industries. Again, banks and insurance companies in general earn high marks for being at a more advanced stage of ERM development – understandably so in light of regulatory constraints and the complexity of their products.

Recent legal and regulatory developments

While no laws, regulations, or bright-line cases require boards to implement formal ERM processes, a number of regulatory and legal developments are redefining directors' duties and potentially suggest a need to reinforce ERM.[3] Here are a few illustrative developments.

- In Delaware corporate law, interpretations of a director's duties of care, loyalty, and good faith (the so-called "business judgment rule") are evolving. In the Caremark case, for example, the court implied that directors are responsible for ensuring the existence of effective compliance and control systems, and that failing to do so could make them liable for losses in some instances.[4]
- The NYSE requires the audit committees of listed companies to "discuss policies with respect to risk assessment and risk management," including their companies' "major financial risk exposures and the steps management has taken to monitor and control such exposures." [5]
- Amendments to the Federal Sentencing Guidelines (2004) place additional process burdens on directors to "exercise reasonable oversight with respect to the implementation and effectiveness of the company's compliance and ethics programs." [6]
- As part of the new securities offering reforms approved by the SEC in 2005, issuers are now required to disclose risk factors in their annual reports and in their 10-K and 10-Q quarterly updates.

ERM as a value-adding function

Perhaps because directors focus foremost on the legal and regulatory issues associated with risk, 31 percent of directors we surveyed still consider ERM programs low-value-adding

3 This section is based on the legal analysis portions of The Conference Board's 2006 report, *The Role of the U.S. Corporate Board of Directors in Enterprise Risk Management*, and is provided with the permission of The Conference Board.

4 In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del Ch. Sept. 25, 1996).

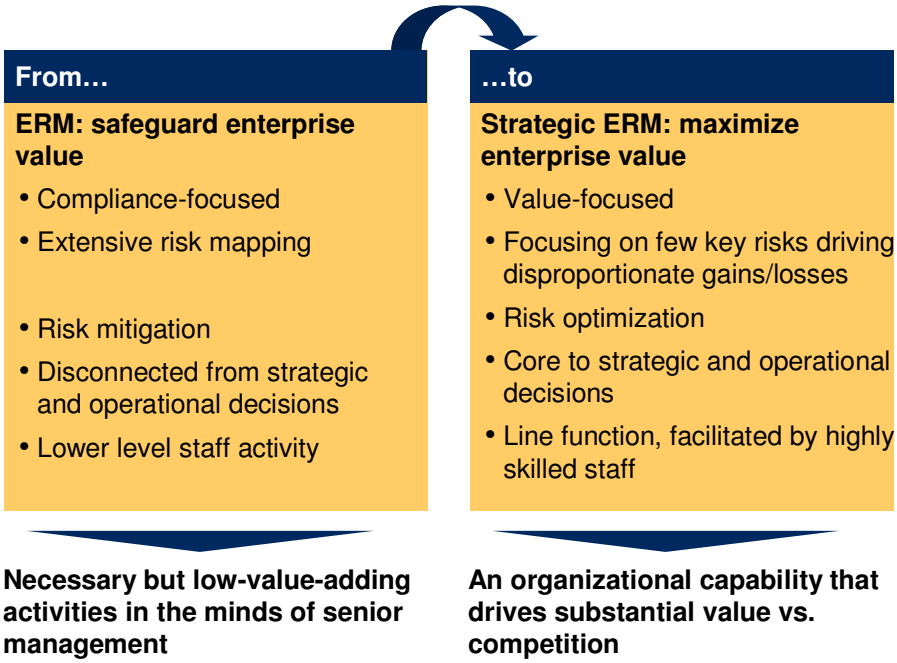
5 Section 303A of the NYSE *Listed Company Manual*.

6 See *2004 Federal Sentencing Guideline Manual*, Chapter Eight ("Sentencing of Organizations"), Amendment 673 (Supplement to Appendix C), at http://www.ussc.gov/2004guid/tabconchapt8.htm.

activities aimed solely at safeguarding enterprise value. At their companies, ERM is driven by staff functions and ends up having little impact on their value-creation agendas. This picture is changing, however, and 39 percent of our surveyed directors now recognizing ERM as a core strategic function.

EXHIBIT 2

The shift to strategic ERM



Boards leading this evolution consider ERM central to managing risk/return trade-offs, one of senior management's highest-value activities (Exhibit 2). Their ERM typically addresses questions such as:

- How much should we invest, and how should we invest, to minimize value losses from extreme risk events (i.e., high-impact/low-probability ones that could destroy business)?
- What level of cash-flow volatility would maximize enterprise value? In other words, how much exposure do we want to unanticipated changes in the business environment that may improve or deteriorate business performance?
- What is the optimal risk/return profile for the company, and how does that translate into business scope and set-up?

Common wisdom is emerging on how to make ERM work

After a slow start and many stories about ERM implementation failures, a consensus appears to be emerging on how to organize an ERM effort and extract value from it. While risks, requirements, and regulations differ significantly across industries and business models, three common themes have emerged: risks should be overseen by the full board, managed by line management, and discussed freely in multiple forums. Additionally, many directors we have advised see board composition as increasingly important for success.

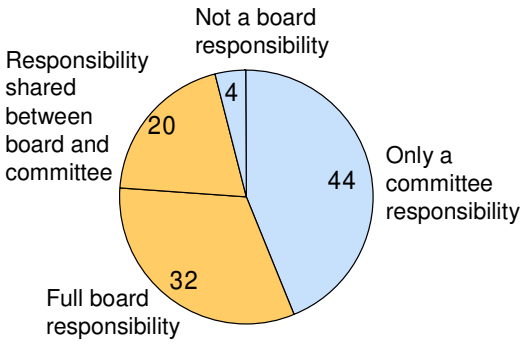
The full board should oversee risks

Over half of the surveyed directors indicated that at least part of the responsibility for risk oversight resides with the full board. The full board should have a certain level of responsibility for ensuring the existence of effective processes for identifying, assessing, and mitigating the company's risks. As well, only 21 percent think there is a need for a separate risk committee (Exhibit 3). But our work and interviews with board directors reveal a fair amount of ambiguity.

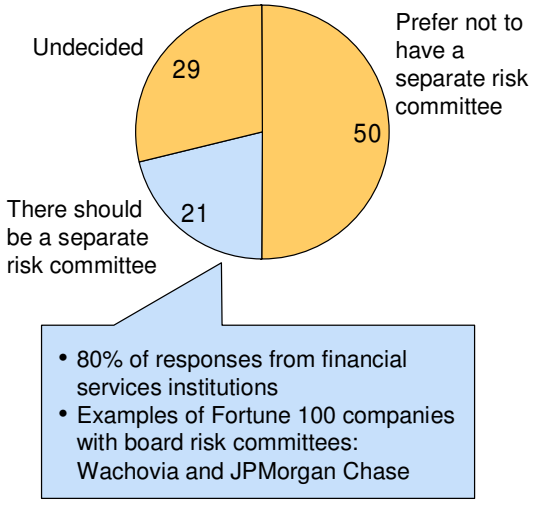
EXHIBIT 3

Many directors believe the full board should oversee risk management

"Who on the board is responsible for risk oversight?"



"Is there a need for a risk committee?"



When asked formally where risk management actually resides in the board, for example, 66 percent of the respondents said they assign risk strictly to the audit committee. Furthermore,

even though most directors say risk discussions take place in virtually every board meeting and executive session, ERM or risk management is rarely listed as an agenda item.

This ambiguity stems partially from different working definitions of risk. Our follow-on interviews made clear that most board members consider compliance-related risk within the audit committee's domain, and business risk (in the broader sense) among the full board's responsibilities. The danger in this ambiguity of definitions is that it may lead some boards to shirk their duties and give their audit committees more risk responsibility than is appropriate.

We are also hearing considerable debate about unburdening audit committees inundated by Sarbanes-Oxley and creating separate risk committees. But is having a separate committee the right answer? Well, . . . that depends.

For financial institutions whose business is all about risk taking, board members might be better served by a risk committee fully devoted to understanding complex risk issues and with specialized expertise that reports its findings to the full board. This structure has become commonplace in many financial institutions (e.g., SunTrust, Capital One, Wachovia, St. Paul Travelers, JPMorgan Chase, Duke Energy).

Conversely, in an oil and gas company, risks are residual. They are not the business's central purpose, as they are in the financial sector, but are connected to the value-generating activity. In these instances, the discussions of risk may not require a separate committee but should occur as various exploration projects are being evaluated by the full board, as well as annually or semiannually during an integrated board-level discussion of risk.

As well, a few institutions have chosen to assign risk oversight to a different committee altogether, one with broader responsibilities and separate from an audit committee (e.g., the MetLife Governance Committee).

Line management should manage risks

Board members may unanimously believe that the overall responsibility for ERM resides with the CEO – who must infuse the business units and line managers with risk responsibility – but they also routinely worry about whether their companies are managing risk appropriately.

Should there be a separate ERM function? Or should risk management be an integrative consideration for each line manager?

One director we interviewed put it bluntly: "You don't want your risks to be managed by a staff person – ultimately line management is accountable if something goes wrong." Our perspective is that risk management is, first and foremost, a line function. Once that is recognized, however, someone still needs to integrate it at the enterprise level, ask the right questions, develop the right reports and frameworks, and facilitate the ERM processes. Additionally, in many risky and heavily regulated businesses (e.g., banking), risk management serves an important control function and is subject to significant regulatory requirements.

ERM accountability should primarily ensure that the risk management process is working: that risks are fully transparent to management and the board, risk tolerances are clearly defined, the right tools are in place to support decision making, and appropriate oversight is provided. Consistent with one director's view that "the role of ERM staff is to educate and train line

management," a centralized ERM supports, trains, and provides tools to line managers who have to manage their risks.

Risk should be included in multiple discussion forums

Our conversations with directors have revealed an overwhelming belief that risk management should be part of a variety of discussions and not confined to the risk portion of the board's agenda.

To get insights into risk, directors are increasingly leveraging their interactions with senior executives (line management and risk officers), rather than relying solely on the reports of the CEO or CFO. Risk-focused directors need honest answers to several questions:

- Does your board truly invite and welcome management to articulate risk issues, even when solutions are not yet clear?
- Is there a sense that management is holding back because the board is not particularly receptive to ambiguity?
- What changes would lead your board to agree with the director we interviewed who declared the advent of the executive session "the single greatest improvement in governance" in the past 10 years?

Many directors stated a preference for focusing risk discussions on specific business issues, rather than high-level generalities about risk. We also found pockets of resistance to making risk processes too formal and bureaucratic.

Our view is that a mixed, nuanced approach will likely yield the best results. Risk should be discussed freely in multiple forums. When management examines new business initiatives, for example, risk and reward should be equally covered. We also believe that there is a need for synthesis which can only be achieved through an integrated process. Moreover, companies with successful ERM processes have reported that such processes are value-adding and increase the management team's – and the board's – understanding of risks and opportunities.

Board composition matters

In addition to holding strong ideas on how their boards should approach risk, the directors we interviewed believe that board composition is a key differentiating factor for ERM success. They agree that the presence of individuals having a mix of backgrounds ensures a needed variety of perspectives on risk issues. As one director stated, "Boards used to be clubby; now they are sharper, more alert, and transparency has increased a lot."

Clearly, the regulatory environment has encouraged board members to take their responsibilities for risk more seriously and to become increasingly willing to challenge one another's perspectives. For many boards, this represents a new and sometimes unexpected mindset.

Recommendations for upgrading a company's ERM capabilities

1. Understand and discuss management's vision for risk management

Board members should invest in learning more about their company's established risk practices and frequently discuss them with management to ensure a steady focus on the target end state for these practices. Understanding the organization's level of risk management sophistication will help the board think through what questions to ask and what answers to expect. For example, a company just beginning its risk management efforts typically can't quantify risk consistently – but it can create a qualitative heat map and provide some quantitative analysis to better describe the nature of each risk.

2. Ask management to obtain an independent assessment of the company's risk management practices

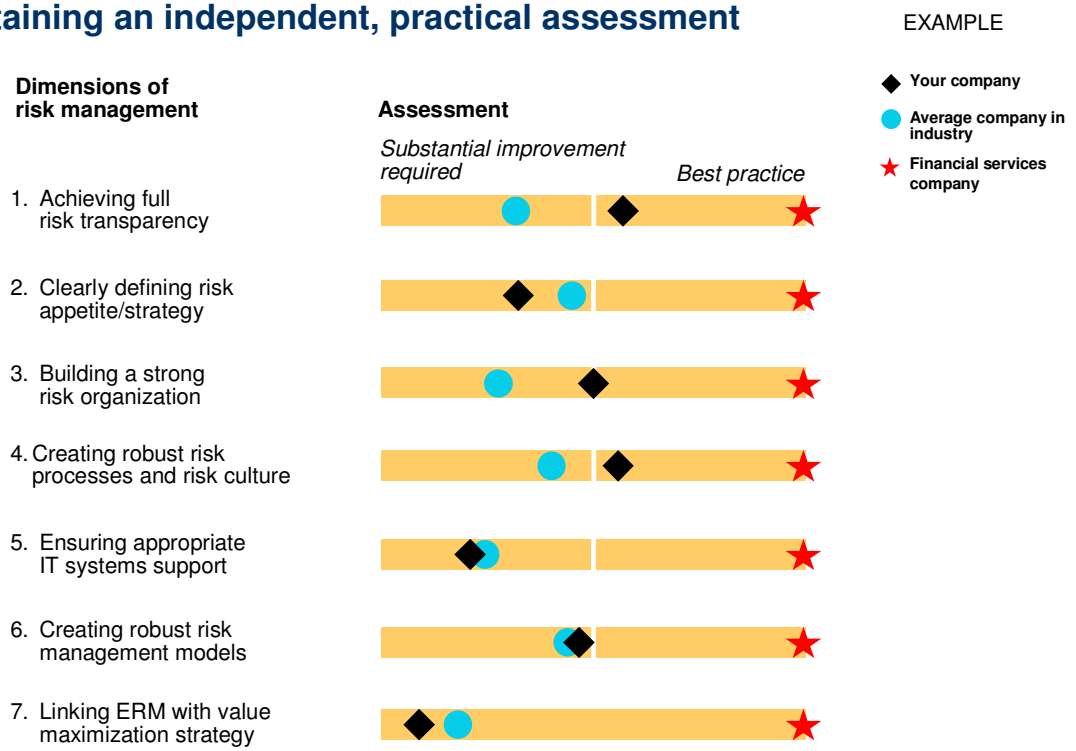
A number of directors found tremendous value in periodic, outside assessments of the company's risk management practices (see Exhibit 4 on the following page). One director commented, "Such a diagnostic can provide real, practical insights for management and, as a board member, you need to know how your company stacks up to peers in the industry and relative to best practice." As expectations with respect to director conduct are evolving, initiating such a review may protect the board from liability suits, as a review demonstrates the board's commitment to ensuring best practices in risk management are implemented at the company.

3. Spend real time with management to get to the core of risk issues

Board members should identify the handful of executives who have the best perspectives on the company's key risks, and then interact with them directly. This is an excellent opportunity to address crucial questions about the risk capabilities within the organization and to diagnose the state of the company's risk management evolution. Understanding management's vision for risk management can help frame the discussions. The sidebar on page 11 shows some of the questions the board should discuss with management.

EXHIBIT 4

Obtaining an independent, practical assessment



4. Put in place a robust board-level risk reporting and review process to ensure the board has full transparency on key risks

The design of board risk reports begins with a clear understanding of what information the board and its committees need to understand and what they are expected to do with this information. What risks does the entire board need to understand? How often does it need to review them? What should be reviewed by the different committees (e.g., finance, audit, risk)? And for what purpose is management asking the board to consider these risks?

The report should prioritize key risk issues and include management's assessment of those risks – e.g., a transparent description of the trade-offs and management's decisions, and their rationale. Finally, the board report should be part of an integrated framework, wherein business unit reports are aggregated into a company-level risk report, and management information flow and reporting are consistent with board reporting.

Institutionalizing the risk review as a formal board process will also help ensure directors are fulfilling their fiduciary responsibilities and their decisions are protected by the "business judgment rule."

Once risk transparency has been established, directors of leading firms suggest discussing how the key risk drivers relate to the company's strategy and returns.

Focus on four topics to get to the core of risk issues

Risk transparency

- What are the key risks the company is facing that the board needs to understand? When and how often does the board need to debate these issues?
- What is the company's aggregate risk-return profile?
- How does the profile compare to competitors' profiles?
- How can these risks affect cash flow, earnings, shareholder value, credit rating, and the company's relationships with other stakeholders (e.g., employees, suppliers, customers)?
- For what purpose is the board asked to consider major risks – e.g., to satisfy fiduciary responsibilities, give permission to management, make another decision?

Risk organization

- Should the board centralize risk oversight into one committee or establish a separate risk management committee?
- How should the charters for the board and the various committees be changed to reflect an increased need for enterprise-wide risk management?
- Does the company have an independent risk management organization with adequate central oversight of risk?
- If yes, how should the board interact with the centralized risk management function? Does the board need more risk management expertise?

Risk strategy

- What is the company's current risk strategy – the types and amounts of acceptable risk, risk-return tradeoffs, link to value creation?
- What role should the board play in setting or guiding the company's overall risk strategy? What information does the board need to do this effectively?
- Is there full alignment between senior management and the board around the company's risk strategy?
- If the company's risk exposure does not align with the stated risk strategy, how can excessive risk be mitigated?

Risk processes

- Does the board receive its own risk management reporting?
- Does the board regularly perform risk self-assessments?
- How can the board ensure that the company's risk management processes remain durable and effective?
- Is there a strong risk culture in the company? How can the board encourage debate and whistle-blowing on risk-related issues?

5. Determine how the risk management process should interact with the strategic planning process

The board should encourage management to find the best way to inject risk thinking into strategic planning. The answer is often to encourage the ERM team's participation in strategic planning. For instance, the team could be involved in assessing the downside risk and the upside potential of an investment or the optimal level of cash flow volatility for the company.

6. Review the competencies of the board in fulfilling its risk oversight duties

Companies should strengthen their boards, if needed, by ensuring they have the right people with a variety of expertise and the proper training. For instance, PNC Bank appointed Stephen G. Thieke, Chairman of RiskMetrics Group, to its board to leverage his top-notch risk expertise, and Conseco appointed Debra J. Perry, a former senior executive at Moody's, to its board to benefit from her expertise in risk assessment.

A few innovative boards have implemented additional practices to increase their risk IQ, such as:

- Conducting risk management training for all new board members
- Dedicating time at each board meeting to discuss important issues (e.g., the implications of the Basel II capital accord on banks)
- Providing more analysis on the company's risk profile and the risk/return nature of decisions.

7. Explicitly review committee structures and charters

To ensure effective oversight of risk, boards must be clear about which committee has board-level responsibility for risk management oversight. A discussion about emerging best practices (as described above) should provide a starting point for this dialogue.

8. Conduct an annual board self-assessment

Best practice boards review the effectiveness of their risk oversight and management processes annually. Some have developed self-assessment tools with questions for rating the board risk management process along a number of important criteria (see Exhibit 5 for sample questions).

EXHIBIT 5

Board self-assessment example

	Not at all 1	2	3	4	Completely 5
A. Oversight – how well does the board understand…					
• The major risks the company faces?	☐	☐	☐	☐	☐
• Alignment of the current risk profile with its risk strategy?	☐	☐	☐	☐	☐
• The risk-return tradeoffs and the risk-adjusted level of value creation of each line of business?	☐	☐	☐	☐	☐
• Any new types of risk assumed as well as material, extraordinary transactions (e.g., acquisitions of low portfolio, off-balance-sheet transactions)?	☐	☐	☐	☐	☐
• Structure and effectiveness of risk management infrastructure at both corporate and BU levels?	☐	☐	☐	☐	☐
• Philosophy, structure, and effectiveness of corporate risk policies?	☐	☐	☐	☐	☐
• Potential conflicts between risk strategy and policies and compensation systems?	☐	☐	☐	☐	☐
• Progress made against commitments made to board?	☐	☐	☐	☐	☐
B. Effectiveness of committee structure					
• Are the committee charters and responsibilities appropriate and shared by all members?	☐	☐	☐	☐	☐
• Is the committee composition adequate?	☐	☐	☐	☐	☐
C. Effectiveness of board meetings					
• Do the board meetings focus on the core issues (as opposed to, for example, the tactical review of nonmaterial transactions)?	☐	☐	☐	☐	☐
• Do all committee members have an adequate understanding of risk management issues?	☐	☐	☐	☐	☐
• Do all committee members contribute productively to the discussion?	☐	☐	☐	☐	☐
• Is the meeting frequency appropriate?	☐	☐	☐	☐	☐
• Do all committee members attend and prepare for board meetings adequately?	☐	☐	☐	☐	☐
• Is the material presented in a way that enables the committees to fully understand critical issues and decision needs?	☐	☐	☐	☐	☐
• Are the discussion materials for the meetings distributed in advance?	☐	☐	☐	☐	☐

* * *

Strengthening a board's approach to risk management starts with an honest assessment of capabilities and a realistic perspective on how current gaps could become problematic, given today's challenging regulatory and legal environments. Fortunately, many boards have made significant progress in developing robust programs. And some have reached a new level, making ERM an offensive – and a defensive – tool that benefits from a more value-focused approach with ERM at the core of strategic decision making.

André Brodeur is a principal in the Montréal office. **Gunnar Pritsch** is a principal in McKinsey's New York office, and Chief Risk and Operating Officer of the McKinsey Investment Office.

McKINSEY WORKING PAPERS ON RISK

1. **The Risk Revolution**
   Kevin Buehler, Andrew Freeman and Ron Hulme

2. **Making Risk Management a Value-Added Function in the Boardroom**
   Gunnar Pritsch and André Brodeur

3. **Incorporating Risk and Flexibility in Manufacturing Footprint Decisions**
   Martin Pergler, Eric Lamarre and Gregory Vainberg

4. **Liquidity: Managing an Undervalued Resource in Banking after the Crisis of 2007-08**
   Alberto Alvarez, Claudio Fabiani, Andrew Freeman, Matthias Hauser, Thomas Poppensieker and Anthony Santomero

5. **Turning Risk Management into a True Competitive Advantage: Lessons from the Recent Crisis**
   Gunnar Pritsch, Andrew Freeman and Uwe Stegemann

6. **Probabilistic Modeling as an Exploratory Decision-Making Tool**
   Martin Pergler and Andrew Freeman