

# Part I

## A Factual Basis

In their contribution, “The Relationship Between Boards of Directors and their Risk Management Organizations,” Michael A.M. Keehner and David R. Koenig provide a fascinating current look into the actual practices of boards and the risk management organizations in their firms. Based on a survey of leading firms, Keehner and Koenig assess the extent to which boards are full participants in the risk management process. For example, a surprising number of boards do not engage in a regular review of the firm’s risk management policy – although the majority do. Further, as is shown by the results of the Keehner–Koenig survey, a significant minority of chief risk officers question whether their boards are sufficiently skilled to understand their firms’ risk management organization and its reports.

Further, in a majority of firms, the risk management organization either does not report to the board or reports to the board only indirectly. Only in a minority of firms is there a board member charged with being familiar with the firm’s risk management organization. These insights, along with many others provided by the survey, give a sobering view of whether corporate boards are sufficiently prepared for the risk management responsibilities that contemporary corporate governance is forcing upon them.



# The Relationship Between Boards of Directors and their Risk Management Organizations *Are Standards of Best Practice Emerging?*

*Michael A.M. Keehner and David R. Koenig*

## Executive Summary

Over the past decade risk management has evolved from a technical discipline focused on specific exposures to an expectation of shareholders, regulators and others affected by the performance of governance at publicly held companies. Various entities, some more effectively than others, have put into place frameworks to define best-practice governance. Further, risk management practices have developed organically at firms, which, albeit to varying degrees, are compatible with these publicly available governance frameworks.

Boards play an important role, not just in the satisfaction of their fiduciary duties, but as the ultimate authority influence in a company's hierarchy. If there is an expectation that employees are engaged in best-practice governance and risk management, to be achieved, it must be modeled from the top.

At an assembly of large company chief risk officers in late 2007, the extent to which top-level practices differ was strongly in evidence. As a follow-up to that meeting a survey of large institutions around the world was conducted, primarily targeting chief risk officers and company directors. Survey results confirm the anecdotal

findings of our roundtable gathering and provide further evidence that a definition of applied best practices of risk management within a governance structure does not yet exist. However, there are patterns emerging in the position of risk management relative to the board, which committees have responsibility for oversight of the risk management organization and the extent to which risk management is used either as an audit and control function or a function for strategic advantage.

Sixty-five firms, across many industries and most among the largest in their industry, participated in our survey. Several companies provided follow-up interviews that provided further background information. Additional data were gathered from public SEC filings.

The full survey report provides substantial detail on the following key findings:

- There is substantial change occurring, bringing about a more robust incorporation of risk management within the governance structure of many organizations.
- There are a wide variety of current approaches to the implementation of risk management within the enterprise governance framework – even between participants in the same industry.
- Meaningfully different approaches to risk/governance implementation exist at the board committee and executive level, the chains of reporting within the executive suite and in patterns of communications to governance structures.
- The audit committee is the most frequent choice for board oversight of risk management, but risk committees are emerging as an important board-level committee.
- Organizational objectives in incorporating risk management within governance structures differ even between participants in the same industry, but they are almost always multifold.
- Most users of risk management as an element of governance agree that loss avoidance and control objectives are to be served, while a smaller number, but still a majority of respondents, identify an objective of securing a competitive advantage through use of this function.

- Some organizations employ ongoing efforts for the promulgation and improvement of governance and risk management practices within their board and employee populations, while a very substantial body of others do not have such capabilities in place.
- The effective communication of risk policies to employees is the most significant task found lacking, leading to possible overconfidence that employees fully understand the intent of such policies.

Interviewees provided examples of specific governance best practices that could be adopted across different industries.

The importance of identifying best practices has become increasingly evident in recent months. For example, CtW Investment Group, a firm that organizes labor union members having more than \$1.5 trillion in pension money into a voice for corporate accountability, sent letters to members of the board of directors of Wachovia Corp. asking for an explanation of how their board had carried out its duty of care related to the acquisition of a mortgage company and additional mortgage exposure just prior to the subprime crisis and threatening to oppose their re-election as directors if satisfactory answers were not given.<sup>1</sup> Shareholders have sued Freddie Mac regarding its risk management practices.<sup>2</sup> Several CEOs and chief risk officers (CROs), including those from some of the largest financial institutions in the world (including UBS,<sup>3</sup> Merrill Lynch,<sup>4</sup> and Citigroup<sup>5</sup>), have been held accountable for their companies' losses in the subprime crisis, indicating that a growing personal liability may be developing in tandem with the search for best practices.

Our study seeks to provide a point-in-time benchmark for boards and senior risk executives as the internal debate continues regarding the appropriate relationship between risk management and governance structure and the objectives for deploying risk management within publicly held companies.

## Background

In October of 2007, at a roundtable held in New York City, around twenty CROs of major US and international financial organizations and the authors discussed, among other things, the interactions between companies' risk management organizations (RMO) and their respective boards of directors.

The roundtable underscored three important conclusions:

- That there was considerable interest among the CROs in how best to facilitate the interaction between the board and the RMO.
- There were a wide variety of philosophies and practices present within the group and there was little consistency in current implementation.
- Many organizations were in the process of examining or had recently examined this interaction.

Since it appeared that the state of affairs was in a period of flux and/or evolution, and to better understand in practice how the alignment of risk management and governance has been established to address the director's fiduciary responsibilities and the enterprise's corporate objectives, the authors decided to conduct a broader study in order to see what insights, trends and notable practices that effort might yield. In this study, we explore the current state of affairs in the implementation of risk management within a representative sample of corporate governance structures in order to determine:

- Which of several possible corporate objectives for deploying risk management are being addressed by the enterprises.
- Whether there are any discernable trends in risk/governance implementation.
- Whether there are any notable best practice innovations that might be worthy of a broader exposure to the governance and risk management communities.

The basis of the analysis contained in this paper is an empirical survey of the CROs and board directors of large companies, as well as a survey of SEC filings, conducted during January and February of 2008.

## Survey Respondent Profile

Sixty-five firms, most of them among the very largest in their industry, responded to our survey requesting information about the relationship between their boards of directors and the risk management organization at their firm, as well as the positioning of risk management in the organizational framework.

**Table 1.1** My company is:

	<i>Response (%)</i>	<i>Response count</i>
Among the largest in our industry	60.0	39
In the largest 25% of firms in our industry, but not among the very largest	16.9	11
Average size for our industry	10.8	7
Smaller than average size for our industry	12.3	8

Table 1.1 shows that 76.9 percent of responses come from companies that are among the largest 25 percent in their industry.

The survey responses were received primarily from CROs, as is shown In Table 1.2.

**Table 1.2** My role is:

	<i>Response (%)</i>	<i>Response count</i>
CEO	1.5	1
CRO/Head of risk management	72.3	47
Head of audit	0.0	0
Chief Financial Officer	1.5	1
Chief Operating Officer	3.1	2
Chief Investment Officer	4.6	3
Board member	7.7	5
Other	16.9	11

Those identifying themselves via the “Other” option include staff in the following positions: enterprise risk management leader, group credit risk director, chief compliance officer, regional head of risk management, head of risk analytics, enterprise risk manager, global risk head, non-executive chairman and head of credit policy.

Table 1.3 shows that the survey respondents represented a large number of industries.

**Table 1.3** My company works in the following industry or industries:

	<i>Response (%)</i>	<i>Response count</i>
Aerospace & Defense	2.0	1
Agriculture, Food & Beverage	2.0	1
Alternative Investments	8.0	4
Banking	40.0	20

(Cont'd)

**Table 1.3** (*Cont'd*)

	<i>Response (%)</i>	<i>Response count</i>
Chemicals	6.0	3
Computer	2.0	1
Diversified Financial Services	14.0	7
Energy	6.0	3
Environment	6.0	3
Government	6.0	3
Healthcare	4.0	2
Industrial Goods & Equipment	6.0	3
Insurance	14.0	7
Manufacturing	4.0	2
Mining & Mineral	2.0	1
Services	2.0	1
Software/IT	2.0	1
Telecommunications & Online		
Services	4.0	2
Traditional Asset Management	8.0	4
Transportation	2.0	1
Utilities	8.0	4
Other	12.0	6

*Notes:* Survey invitees were selected because each had evidence of an existing risk management organization. This selection decision necessarily introduces a bias toward acceptance of risk management on the part of responding companies. Except where specifically cited, the rest of this report contains analysis and results that are based upon the data of those respondents, indicating that they are either among the largest in their industry (39 responses) or among the top 25 percent in their industry (11 responses), a total of 50 responses. We note also that there is a concentration of respondents within financial services. Where survey response results for non-financial companies illustrate striking differences from those of financial service firms, they are highlighted in the report that follows.

## A Brief History of Convergence

The subjects of risk management and governance are popular topics. In corporate circles, the practice of the formal identification and management of risks has been accelerating since the mid-1990s, when a series of corporate mishaps focused attention on the potential value of having an organizational function identify and attempt to characterize the nature of risks which an enterprise might undertake and/or encounter. The premise of this

movement was that managers and boards of directors, as owner-surrogates, might be better prepared to make intelligent choices between competing investments on one hand, and forms or degrees of risk on the other. Such analysis was believed to foster the selection of appropriate combinations of risk and return, avoiding – or at least mitigating – the potential occurrence of others' missteps.

Similarly, since the 1980s considerable attention has been paid to the subject of corporate governance. This has led to a growing clarity on the distinctions, conflicts and tensions between corporate managers and board of directors as owner-surrogates. Another leg of the owner–manager–director triangle, the responsibilities of directors to shareholder constituents, has also received considerable attention and clarification in both legal studies and countless court cases.<sup>6</sup>

On a broad plane, the inevitable confluence of these developments is obvious. The actual intersection of governance and risk management, however, is not so easy to isolate; nor is the optimal mechanism by which to accomplish it necessarily clear.

## **Directors' Duties Drive Interest in Risk Management**

The general expectation of responsible behavior on the part of boards of directors and managers by shareholders and regulators is usually expressed as corporate governance. Corporate governance is defined by the OECD as:

The system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation such as the Board manager shareholders and other stakeholders and spells out the rules and procedures for making decisions and corporate affairs. By doing this it also provides the structure through which the company objectives are set and the means of attaining those objectives and monitoring performance (OECD, 2004; available at <http://www.oecd.org/dataoecd/32/18/31557724.pdf>).

Over the past twenty years, the practice of risk management has developed from a technical discipline, focused primarily on specific areas of exposure, to an expectation held by investors, regulators and stakeholders that risk management will be a core element of the way in which a business is run.

Businesses exist to take risks for the benefit of their shareholders. As a result of their their geographic dispersion, disintermediation and varying

interests, shareholders are relatively powerless to affect the way in which a company is managed. However, under our legal systems and traditions, their proxy can be found in the board of directors. Directors are elected by shareholders and are given certain powers, including the abilities to hire, fire, and evaluate management and to set corporate strategy. Legally, they are the ultimate decision makers within the corporation, bearing a fiduciary duty to protect and serve the interests of the shareholders.

Directors' fiduciary responsibilities include both a Duty of Care and a Duty of Loyalty to their shareholders.<sup>7</sup> These are often expressed in terms of a duty to act in the best interests of the corporation, rather than their own personal interests, and to be diligent, thoughtful, and professional in their oversight of the corporation. One manifestation of these duties is to set standards for corporate and employee behavior and another is to establish systems and controls through which to monitor and manage the corporation's opportunities, risks and operations.

## **Arguments for the Implementation of Risk Management**

From the point of view of the corporate directors, the promise of isolating and managing risk, and in particular the promise of global enterprise solutions, makes it inevitable that companies should avail themselves of the technology of risk management – and for a whole variety of reasons. These range from the very pragmatic to the extremely esoteric. They also imply a variety of governance structures which might be deployed to effect the practice of risk management in any given corporate framework, depending upon the mix of objectives sought.

Certainly a body of financial thinking based upon theories of capital structure, efficient markets, and portfolio management does provide some reasons for effecting risk management within a framework of corporate governance. On the financial side, the usual reasons for implementing risk management include:<sup>8</sup>

- Reducing the costs of financial distress and bankruptcy.
- Developing financial plans and funding investment programs.
- Stabilizing cash dividends.

Clearly, each one of these issues is in the realm of a board-level consideration. And the recognition of financial agency theory contributes further

governance-related reasons to manage risk within a governance framework; mindful of the fact that risk diversification options are starkly different for shareholders and managers.<sup>9</sup>

- Better aligning the interests of managers and shareholders.
- Designing appropriate compensation programs.

On yet another level, a director's fiduciary responsibilities provide more reasons to consider risk management as it bears on improving the execution of their duties to be informed and to make decisions that are loyal to the interests of their shareholder constituency.<sup>10</sup> Certainly the hazard of failing to avail oneself of a source of potentially relevant decisional information from a rapidly developing management technology alone raises considerations of risk management implementation. There are also parallel considerations that stem from board duties to ensure that compliance standards are met, and systems and controls are implemented and effective which may make a risk management infrastructure attractive.<sup>11</sup> And last but not least, there is the completely pragmatic consideration that a failure to implement risk management might impact a corporation's value in the eyes of various stakeholders and marketplaces.

Thus a board that is seeking to make use of the risk management tool might select from an array of objectives: some will have a bear on strategic matters, others will add capabilities relating to enhanced corporate discovery and fact-finding, while still others are focused more on the areas of added compliance and verification. The foregoing all implies that a variety of competing rationales will lie behind the actual design of a risk management organization, which are presumably reflected in the choices which boards have made in implementing their own unique approaches to risk management.

### **Existing Frameworks: A Bifurcation of Risk Management Choices – Compliance or Value Creation?**

Emerging frameworks for best practice corporate governance and risk management include several structures designed by various organizations that are involved in the risk management of corporations and financial systems. Among the most widely recognized are the COSO/Treadway Commission standards<sup>12</sup> which have been developed primarily by the accounting and internal audit profession; Sarbanes–Oxley, a legislative and regulatory response to the corporate fraud cases of the late 1990s; and

newer work in the area of governance risk and compliance (GRC), as evidenced by the OCEG framework.<sup>13</sup>

But perhaps the most widely known current approach to wide-ranging risk management is identified by the term enterprise risk management (ERM). Unsurprisingly, ERM means different things to different groups, ranging from very limited applications in IT – where ERM is designed primarily as a control to ensure the stability of an IT infrastructure – to much broader applications as defined by the actuarial and financial professions encompassing every aspect of risk that a corporation faces. A broader vision of enterprise risk management, as established by authors such as James Lam,<sup>14</sup> is focused on the value which might be added through the adoption of a holistic approach to risk management. In turn, this vision has come to dominate discussions of governance, risk and whether or not value is driven by risk management as a practice.

Lam and others position enterprise risk management and corporate governance as being fully integrated into the normal process of business decision making. Similarly, the governance and risk management principles as defined by the ANZ-4360 standard<sup>15</sup> and implemented in the Australian and New Zealand markets put governance in a flexible format that provides strategic services to various industries and organizations. Frameworks such as COSO, however, tend to put enterprise risk management and governance into a more rigid and compliance-focused focus. This bifurcation between risk management as a control capability (audit, for example) and risk management as a strategic utility at the executive and policy levels may have profound implications for the ability of risk management organizations and governance structures to create shareholder value, since the need for risk-related information is accentuated in the carrying out the functional duties of executive and directors and also by statutory demands.

Ultimately, the question for any board of directors returns to the purpose of a risk management organization within the company. Is its primary intention to be supportive, or even an enhancement of the firm's ability to pursue its strategic objectives? Is it intended to be more of a defensive tool? Or is it viewed and positioned to focus more on regulator compliance? Can an RMO be both control-oriented and strategically focused?

## **Substantial Change is Occurring in Risk Management and Governance Schemes**

It is clear that the general state of board and risk management organization relationships is currently in flux as organizations achieve a better

understanding of their needs and move to adapt risk management to contemporary demands. In our survey respondents were asked about significant changes in risk management and governance practices over the course of the past two years.

Below is a sample of some of the most significant responses:

- Our risk committee is now looking at risk management with more granularity.
- The board is applying a risk/return measure more consistently across the institution.
- Basel II is a big priority for the firm and has garnered more attention.
- The board has increased the level of detail and oversight.
- The board originally didn't have the finance committee overseeing risk policies.
- The amount of information sent to the audit committee has decreased somewhat.
- Better transparency at the Risk Committee on risk of the company – now in a better position to make their own judgment on the risk of the company with this transparency.
- Report design and content has been changed in order to make them more meaningful for the board.
- The board has added new members that were quite knowledgeable about risk management.
- The combined audit and finance committees now meet together when they used to be independent (two times each year) – the agenda for these meetings is set by the board and the chairs of both committees.
- More direct reporting from the CRO to the board.
- We've created a new board-level risk committee.
- Our chief risk officer's position was created two years ago.

## Benchmarking Results

In our survey design and the analysis of the data, there are three core lines of inquiry related to the governance purpose and deployment of a risk management organization and emerging applied best practices. These are:

1. Are large companies exercising risk management as an element of governance?

2. How is risk management implemented within the enterprise governance framework?
3. Are there ongoing efforts for the promulgation and improvement of governance and risk management practices?



In the following sections, we have identified the survey data which bear on the answers to these and important subsidiary questions. Together, these answers provide an important guide to the present state of the art in the implementation and use of risk management within existing governance structures.

*Question 1 Are large companies exercising risk management as an element of governance?*

Three survey questions shed light on this issue:

*A. Are effective policies in place?* The first is the question of whether the enterprise has a risk management policy, and whether or not that policy is understood within the organization. In our survey 90 percent of respondents report that their company has a formal risk management policy (see Table 1.4).

**Table 1.4**

DOES YOUR COMPANY HAVE A RISK MANAGEMENT POLICY?		Response (%)	Response Count
Yes		90.0	45
No		10.0	5

We must emphasize, however, that the existence of a risk policy is not necessarily the same as having a risk policy that is understood throughout the organization. This is particularly the case since the majority of respondents were CROs who often have direct responsibility for such promulgation. In fact, psychological literature suggests that any expectations that risk management and conduct policies are well understood is likely to be overstated by management.<sup>16</sup> (More on this subject is discussed in the Appendix at the end of this paper.)

*A.1. Is the policy promulgated from the highest levels in the corporation?* The board tends to play an important role in the oversight of the risk management policy, with just 7 percent of those with a risk management

policy indicating that their board does not review it. This positions the risk management policy at the top of the corporate hierarchy. It is therefore represented to employees as an important document in the process of effective governance of the company.

At the board level, one would assume that there existed a broad level of understanding about the policy, its origins and its intent. Yet while 76 percent of respondents feel that their board has sufficient skill to understand their risk management organization, policies and reports, one in nine feels that they do not.

**Table 1.5**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
The board regularly reviews the risk management policy	40.0% (18)	44.4% (20)	8.9% (4)	6.7% (3)	0.0% (0)	45
The board, as a whole, is sufficiently skilled to understand our RMO and its reports	31.1% (14)	44.4% (20)	13.3% (6)	11.1% (5)	0.0% (0)	45

One generally accepted tenet of governance is the provision of sufficient competencies in critical areas of the corporation, including the board. At the board level, this means that members must be able to understand the business and the environment within which the enterprise operates and also that the board should be composed in a manner such that sufficient independence and expertise exist to offer a competent evaluation of the business structure and environment in which the corporation operates and to formulate appropriate responses. Certainly, the risks the firm is facing as reported by a risk management organization form a significant part of that business environment awareness; and by that measure, the fact that nearly 25 percent of respondents question whether there is a sufficient competency on their respective boards is worthy of note.

*A.2. Are risk policies understood throughout the enterprise?* Most respondents feel that their risk management policies are understood, but only 27 percent feel strongly that their policies are well understood throughout the organization.

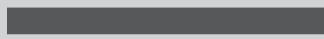

**Table 1.6**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
Our risk management policy is well understood throughout the organization	26.7% (12)	53.3% (24)	11.1% (5)	8.9% (4)	0.0% (0)	45

We wish again to emphasize that typically there is an overconfidence on the part of managers that policies formulated and issued from executive levels are well understood.

*B. Has the risk management responsibility been clearly assigned? If so, how?* The second question concerns whether or not the enterprise has formalized the responsibility for risk management. While there are in principle many forms such assignment might take, the vast majority of these reporting companies have established a single point of risk management within the management hierarchy. More than 82 percent of those who responded to our survey indicate that their firm does have a chief risk officer (CRO) or other head of risk management for the entire organization.

**Table 1.7**

DOES YOUR COMPANY HAVE AN ENTERPRISE-WIDE CRO?		Response (%)	Response Count
Yes		82.0	41
No		18.0	9

Of those indicating that they did not have a chief risk officer, the responses came from the following industries:

Insurance (2)	Financial Services (2)
Banking (1)	Alternative Investments (1)
Computer (1)	Software/IT (1)
Chemicals (1)	

It is interesting to note that all of these responses came from firms identified as being among the very largest in their respective industries. At those firms with no CRO, responsibility for risk management resided with the:

CEO (2)	CFO (2)
COO (1)	CIO (1)
CIO/CFO jointly(1)	“Various people” (1)
Investment Committee (1)	

*C. What organizational objectives are being pursued through the management of risks?* Our results show that firms are indeed pursuing risk management as a strategic objective (to achieve competitive advantage), for loss avoidance and as a control. Further, compliance with regulations is a strong driver of risk management’s purpose at more than one-third of the firms in our survey. Only a very small number of firms report having risk management exist primarily to serve their internal audit needs. Note, however, that these responses are primarily from CROs, and that the recitation of corporate objectives reported here may or may not be fully representative of the views of the boards of directors who established the risk management function and its objectives.

**Table 1.8**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
The primary purpose of our RMO is for competitive advantage	23.9% (11)	32.6% (15)	23.9% (11)	15.2% (7)	4.3% (2)	46
The primary purpose of our RMO is for regulatory compliance	8.7% (4)	26.1% (12)	28.3% (13)	28.3% (13)	8.7% (4)	46

(Cont'd)

**Table 1.8** (Cont'd)

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
The primary purpose of our RMO is for loss avoidance	15.2% (7)	54.3% (25)	19.6% (9)	4.3% (2)	6.5% (3)	46
The primary purpose of our RMO is for control	21.7% (10)	43.5% (20)	23.9% (11)	8.7% (4)	2.2% (1)	46
The primary purpose of our RMO is for internal audit	0.0% (0)	13.0% (6)	23.9% (11)	43.5% (20)	19.6% (9)	46

It is interesting to note that as is reported through this survey, in respect of their risk management organizations the domains of objective pursuit are not exclusive with these boards of directors. In other words, firms that feel that they may be pursuing risk management primarily for a strategic purpose often note that they also pursue it for control purposes; and, conversely, those who see the function as primarily supporting information and/or control purposes in some cases also identify it as having some strategic role.

These responses are detailed further in the following paragraphs. Where respondents indicated that they either “agree” or “strongly agree” with a statement this was taken as an affirmation of an objective they held for their risk management unit, whereas the responses “strongly disagree” or “disagree” were taken as indicative of an objective they did not hold for the risk management unit.

Of those respondents who indicated by “strongly agreeing” or “agreeing” that the primary purpose of their risk management organization was for competitive advantage, a majority also indicated it had the additional primary purpose of loss avoidance and control.

**Table 1.9**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
The primary purpose of our RMO is for competitive advantage	42.3% (11)	57.7% (15)	0.0% (0)	0.0% (0)	0.0% (0)	26
The primary purpose of our RMO is for loss avoidance	19.2% (5)	50.0% (13)	15.4% (4)	7.7% (2)	7.7% (2)	26
The primary purpose of our RMO is for control	23.1% (6)	42.3% (11)	23.1% (6)	7.7% (2)	3.8% (1)	26
The primary purpose of our RMO is for regulatory compliance	11.5% (3)	23.1% (6)	30.8% (8)	23.1% (6)	11.5% (3)	26
The primary purpose of our RMO is for internal audit	0.0% (0)	15.4% (4)	30.8% (8)	30.8% (8)	23.1% (6)	26

Among those respondents who indicated that the primary purpose of their risk management organization was for control, more than 80 percent said that it had an additional primary objective of loss avoidance, which is not a surprising pattern. However, a majority of the same respondents said that risk management was also aimed at achieving competitive advantage.

**Table 1.10**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
The primary purpose of our RMO is for control	33.3% (10)	66.7% (20)	0.0% (0)	0.0% (0)	0.0% (0)	30
The primary purpose of our RMO is for loss avoidance	23.3% (7)	60.0% (18)	13.3% (4)	0.0% (0)	3.3% (1)	30
The primary purpose of our RMO is for competitive advantage	26.7% (8)	30.0% (9)	20.0% (6)	16.7% (5)	6.7% (2)	30
The primary purpose of our RMO is for regulatory compliance	6.7% (2)	33.3% (10)	30.0% (9)	23.3% (7)	6.7% (2)	30
The primary purpose of our RMO is for internal audit	0.0% (0)	16.7% (5)	36.7% (11)	33.3% (10)	13.3% (4)	30

From the data, it would seem that firms believe a solid foundation of loss avoidance and control is necessary in order to be able to pursue risk management for competitive advantage.

And, finally, regulatory compliance was identified as a primary driver of risk management organizations by 16 of the 46 respondents to this question; but again, it was generally not to the exclusion of the pursuit of additional objectives of competitive advantage, control or loss avoidance.

**Table 1.11**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
The primary purpose of our RMO is for regulatory compliance	25.0% (4)	75.0% (12)	0.0% (0)	0.0% (0)	0.0% (0)	16
The primary purpose of our RMO is for loss avoidance	12.5% (2)	68.8% (11)	18.8% (3)	0.0% (0)	0.0% (0)	16
The primary purpose of our RMO is for control	18.8% (3)	56.3% (9)	25.0% (4)	0.0% (0)	0.0% (0)	16
The primary purpose of our RMO is for competitive advantage	18.8% (3)	37.5% (6)	25.0% (4)	12.5% (2)	6.3% (1)	16
The primary purpose of our RMO is for internal audit	0.0% (0)	25.0% (4)	25.0% (4)	50.0% (8)	0.0% (0)	16

**Comments from Respondents in Respect of Organizational Risk Management Objectives**

“The ownership and management of risk falls to the business and business leaders. Our RMO facilitates the program that helps them identify, define, assess, and if necessary mitigate, control, and improve the risk management capabilities within the business. The control environment is reviewed via our Internal Audit plan and SOX requirements; however, the RMO assesses this aspect of risk when determining what mitigation efforts are needed.”

“The primary purpose of our RMO is to ensure there are no surprise losses, and to ensure that we are properly compensated for the risks we take.”

“The primary purpose is to drive economic growth and preserve long-term capital.”

*C.1. Is risk management an exercise in due diligence?* Another relevant question in this study of the interaction and objectives of the board of directors and the RMO is to what degree the risk management organization is perceived to be an extension of the board’s duties to be diligent and well informed on the condition of the corporation (their “due diligence” obligations). In our survey, 50 percent of respondents agreed that their risk management is a due diligence process for the board. However, more than 20 percent disagreed with this assessment.

**Table 1.12**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
Risk management is a due diligence process for our board	8.7% (4)	41.3% (19)	28.3% (13)	15.2% (7)	6.5% (3)	46

Finally, as a further indication that these corporations were quite diverse in their overall views of the purpose of their risk management organizations, more than one in three did not regard risk management as being a managerial/administrative responsibility in their organization, with a roughly equal number saying that it was such a responsibility. We also offer the possibility that these statements are open to diverse interpretations, but we note the responses as a point of possible interest to readers.

**Table 1.13**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
Risk management is a managerial/administrative responsibility	10.9% (5)	26.1% (12)	28.3% (13)	21.7% (10)	13.0% (6)	46




*Question 2 How is risk management implemented within the enterprise governance framework?*

Here we examine responses which bear on how these large companies have chosen to position risk management within the governance structures used to manage their enterprises. The authority influence of the risk management organization is highly dependent upon its placement within the firm's hierarchy.

*A. Is there a direct involvement with risk management on the part of the board of directors? A.1. Is there a direct reporting relationship to the board of directors?* The growing significance of risk management to the governance structures at these companies is further evidenced by data showing that among large companies more than 78 percent report, either directly or indirectly, to the board of directors.

The strongest governance connection, a direct board reporting relationship, is evident in 37 percent of the respondents, while 41 percent have some intermediary in the management structure interposed between the RMO and the board of directors. The remainder, comprising only 22.4 percent of these companies, have no relationship to the board.

**Table 1.14**

DOES YOUR RISK MANAGEMENT ORGANIZATION REPORT TO THE BOARD?		Response (%)	Response Count
Does not report to the board		22.4	11
Reports to the board directly		36.7	18
Reports indirectly		40.8	20

In this sample, the most common route for indirect reporting is through the CFO (9), although for nearly as many, the CRO reporting route is

through the CEO/president/general manager (7). Other routes found were through the investment committee (1), the chief counsel (1), the audit committee (1) and the executive committee (1).

Another generally accepted tenet of governance is the preservation of open and uninterpreted communications channels for important auditing and control functions so as to insure the flow of independent facts and judgments to governance authorities. In recent times independent board reporting relationships for internal audit groups have been the most conspicuous form of this communications protection on the part of directors. Those taking part in this survey provide us with one assessment of whether the risk management organization also has an independent route to the board of directors. As shown above, of the large firms, only 37 percent of the risk management organizations report directly to the board. However, through our interviews and also through our own anecdotal experience, we believe this to be a substantial growth from the norm of five to ten years ago, with a particular acceleration in independent board reporting for risk management happening over the past few years. In some instances we encountered other forms of organizations taking steps to insure that risk management communications channels to the board would not be interfered with by management fiat.

*A.2. Is there a single individual accountable for risk management on the board of directors?* Another measure of governance seriousness of purpose concerning risk management matters is whether or not there is a single board-level individual with responsibility for being familiar with the risk management organization of their firm. We note that only 31 percent of firms report that such clear accountability is in place, even among those firms selected for our study, which we assume are likely to be more advanced in their approaches.

**Table 1.15**

IS THERE A SINGLE INDIVIDUAL ON THE BOARD WITH RESPONSIBILITY FOR BEING FAMILIAR WITH THE RISK MANAGEMENT ORGANIZATION OF THE FIRM?		Response (%)	Response Count
Yes	██████████	31.3	15
No	████████████████████	68.8	33

*B. What is the governance committee structure being used at the board of directors level to manage these enterprises and to effect governance broadly?* Over time, organizations have evolved a set of board committees they have considered necessary to exercise their governance responsibilities. Some of these are mandated by various regulators and supervisory agencies while others have come into being through choice. Overall, within the population of committees which these large enterprises currently use to exercise governance broadly, an audit committee can be found at nearly 90 percent of respondent firms, while a risk committee exists at just 26 percent:

**Table 1.16**

Range of Committees Present in Respondents' Boards

Audit	86.0%
Executive	56.0%
Nominating	40.0%
Governance	40.0%
Management	38.0%
Risk	26.0%
Finance	14.0%
Compensation	6.0%
Credit	4.0%

*B.1. Which board committee has been assigned the primary oversight responsibility for risk management?* Presumably these organizations have made a choice in selecting the most appropriate board committee to exercise the risk management oversight functions after some consideration of issues, including functional similarities, the available talent, and the anticipated volume of effort. In some cases, they have selected an existing committee to assume this responsibility, and others have formed (often recently) a new committee to oversee the risk function. The following table indicates where this responsibility has been vested.

**Table 1.17**

Board Committee Having Primary Oversight Responsibility for Risk Management

Audit	31%
Risk	17%
Management/Executive	13%
Finance	4%
Governance	4%
Risk Policy Capital	4%
Credit	4%
BoD	4%

There was some consistency among respondents as to where the risk management organization reported to the board of directors. More survey respondents firms place oversight of the risk management organization with the audit committee than with any other board committee. Eight respondents (about 17 percent of these companies) indicate the existence of a board-level risk committee or risk management committee that has the ultimate oversight responsibility for risk management.

The executive (or management) committee of the board is the third most common reporting location and is particularly evident among the smaller respondents in this sample of large and very large companies. One or another of these three board committee location choices was made by more than a majority of the survey group.

Beyond the foregoing, it is difficult to discern much consistency in the choices made by these respective companies. If anything, the assignments probably reflect a combination of assessments of company-specific issues, board member talents and some reflection of an uncertainty about where this assignment might ultimately reside most effectively. The minority not choosing one of the three committees above vest the responsibility for risk management oversight in a variety of different board committees. In some instances, the risk management assignment is added to a pre-existing standing committee which was deemed appropriate for this new responsibility for company-specific reasons, while still others represent an expanded former committee with a new name. Some companies have adopted a dual reporting scheme and others assign the duty to the board as a whole; both probably reflecting the widespread applicability of RMO information and considerations. Finally, some companies have delegated the responsibility for risk oversight to the CEO or chairman alone in their capacity as a board member. In general, this dispersion can probably be seen as evidence that the board of directors' interface with the risk management organization has yet to be settled into a widely acceptable pattern, and the relationship evolution will continue as functional demands, potential regulations, new studies and best practices become evident.

**Table 1.18**


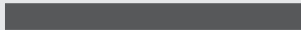



<b>Board Committee Responsible for Risk Management in Large Companies</b>	<b>Financials</b>	<b>Non-Financials</b>	<b>Total Sample</b>
Executive (Management) Committee	6		6
Audit Committee	12	3	15

Risk Committee	8		8
Audit and Risk Management Committee	1		1
Risk and Finance Committee	1		1
Risk Management & Compliance	1		1
Risk Policy Capital Committee	2		2
Finance Committee		2	2
Credit (Credit Risk) Committee	1	1	2
Governance (and Nominating) Committee	2		2
Board of Directors as a Whole	2		2
Chairman/CEO	2		2
Dual Reporting Schemes:			
Audit + Finance Committee(s)		1	1
Risk + Audit Committee(s)	1		1
Finance, Credit + Board as a Whole	1		1
Audit + Investment and Capital Committee(s)	1		1
Total Responses	41	7	48

It is worth noting that the multiplicity of objectives cited as reasons for deploying risk management within a governance structure are also reflected in these committee choices. In particular, the divergence between audit-like risk functionality and strategic risk management functionality (mentioned in an earlier paragraph) is probably very influential in some of the choices companies have made between audit (and similar) committees as the appropriate venue for risk; and other choices, like newly-formed risk committees and executive committees, which may be more appropriate for strategic or operational committee work. This dichotomy of functionality was best highlighted by one respondent who made the distinction that their audit committee deals with “what has happened,” while their risk committee deals with “what could happen.”

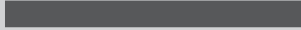
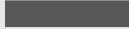
*B.2. How frequently does this primary board committee meet to exercise its oversight?* There is a large amount of variability in the frequency of meetings held by the board committee with responsibility for risk oversight. Quarterly meetings are most typical, but more frequent meeting cycles are also used by many of these respondents. Of those answering “Other,” most reported meeting between six and 10 times per year, while 22.7 percent report that they meet on a monthly basis.

**Table 1.19**

HOW MANY TIMES A YEAR DOES THE BOARD COMMITTEE HAVING RISK MANAGEMENT ORGANIZATION OVERSIGHT RESPONSIBILITY MEET?		Response (%)	Response Count
Monthly		22.7	10
Quarterly		59.1	26
Twice each year		11.4	5
Annually		2.3	1
Only as needed		4.5	2
Other			9

When these committees meet, in more than 80 percent of the cases, the chief risk officer or person responsible for risk management organization attends:

**Table 1.20**

DOES THE CRO OR THE PERSON RESPONSIBLE FOR RISK MANAGEMENT ALWAYS ATTEND MEETINGS OF THIS COMMITTEE?		Response (%)	Response Count
Yes		81.6	40
No		18.4	9

Of the 18 percent who say that the CRO does not attend, nearly 90 percent indicated that someone else in senior management attends who is responsible for risk management. Typically this was the CEO, the CFO or the Chief Counsel.

*C. Do other board committees take an interest in risk management activities even where there is another committee primarily responsible for the risk management function?* The response to this question was somewhat surprising as many board committees do take an active interest in risk management results, even where there is a primary committee with

board-level oversight responsibility present. This may be a function of the relative novelty of the assignment of risk management oversight duties within the board structure, overlaps in committee charter definitions, an acknowledgment of the pervasive nature and perceived relevance of risk management data or one of many other factors which are generally outside the scope of this study. Nevertheless, the degree of overlapping interest and reporting requirements is surprising, since the head of risk management will typically meet with a number of committees, as Table 1.21 indicates.

**Table 1.21**

WITH WHICH OTHER BOARD COMMITTEES (OTHER THAN THE PRIMARILY RESPONSIBLE COMMITTEE) DOES THE CRO OR HEAD OF RISK MEET (AND HOW OFTEN)?		
	Yes	No
Audit Committee	83.7% (36)	16.3% (7)
Executive Committee	55.6% (15)	44.4% (12)
Management Committee	50.0% (11)	50.0% (11)
Governance Committee	26.3% (5)	73.7% (14)
Nominating Committee	6.3% (1)	93.8% (15)

**Table 1.22**

HOW FREQUENTLY?	Monthly	Quarterly	Twice each year	Annually	Only as needed
Audit Committee	8.6% (3)	42.9% (15)	25.7% (9)	11.4% (4)	11.4% (4)
Executive Committee	50.0% (8)	18.8% (3)	0.0% (0)	12.5% (2)	18.8% (3)
Management Committee	54.5% (6)	36.4% (4)	9.1% (1)	0.0% (0)	0.0% (0)
Governance Committee	20.0% (1)	40.0% (2)	20.0% (1)	0.0% (0)	20.0% (1)
Nominating Committee	0.0% (0)	100% (1)	0.0% (0)	0.0% (0)	0.0% (0)

*D. How are risk management reports circulated within the governance organization?* Much like the results reported above, several board committees receive regular reports from the risk management organization in addition to the committee with primary responsibility:

**Table 1.23**

WHICH BOARD MEMBERS RECEIVE REGULAR REPORTS FROM THE RISK MANAGEMENT ORGANIZATION?		
	Yes	No
Board Audit Committee Members	90.9% (20)	9.1% (2)
Board Risk Management Committee Members	88.9% (16)	11.1% (2)
All Board Members	86.2% (25)	13.8% (4)
Board Governance Committee Members	71.4% (5)	28.6% (2)
Board Executive Committee Members	66.7% (8)	33.3% (4)
Board Management Committee Members	57.1% (4)	42.9% (3)
Board Nominating Committee Members	40.0% (2)	60.0% (3)

The frequency of these reports varies widely:

**Table 1.24**

HOW OFTEN ARE THESE REPORTS DELIVERED?							
	Daily	Weekly	Monthly	Quarterly	Twice each year	Annually	Response count
Board Audit Committee Members	0.0% (0)	0.0% (0)	10.5% (2)	73.7% (14)	10.5% (2)	5.3% (1)	19
Board Risk Management Committee Members	0.0% (0)	0.0% (0)	40.0% (6)	60.0% (9)	0.0% (0)	0.0% (0)	15

All Board Members	4.2% (1)	0.0% (0)	41.7% (10)	45.8% (11)	0.0% (0)	8.3% (2)	24
Board Governance Committee Members	0.0% (0)	0.0% (0)	66.7% (2)	33.3% (1)	0.0% (0)	0.0% (0)	3
Board Executive Committee Members	0.0% (0)	12.5% (1)	50.0% (4)	25.0% (2)	0.0% (0)	12.5% (1)	8
Board Management Committee Members	0.0% (0)	33.3% (1)	66.7% (2)	0.0% (0)	0.0% (0)	0.0% (0)	3
Board Nominating Committee Members	0.0% (0)	0.0% (0)	0.0% (0)	100.0% (1)	0.0% (0)	0.0% (0)	1

We also asked whether the risk management organization communicates with the entire board of directors. More than three-quarters reported that the RMO gives regular briefings to the entire board, but a full 24 percent have no such direct communication with the entire board of directors.

### Questions that Board Members Ask of Risk Managers

We asked our interviewees if the board members asked any particular questions that seemed to stand out for their importance or effectiveness in terms of the oversight of the risk function. Their responses highlighted several areas of focus:

- “How do we know that everything is under control?”
- “How do current headlines or risks influence the risk to our business plan?”
- They know that mistakes in business strategy will be the end of our company and they focus on this aspect of risk.


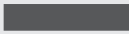
- They are now focused more on liquidity and funding than in the past and ask good questions on this.
- They challenge the quality of the risk management function's radar report.
- They challenge the RMO metrics and quantitative methods and assumptions.
- They vary the amount of time they spend, and points on which they go into greater detail – they don't ask for great detail every time, but the RMO must be prepared in case they do.
- The board regularly asks two questions about the value of the RMO: First, "Are we driving value?" Second, "Are we a reporting function only?"

*Question 3 What is the level of ongoing promulgation and improvement of governance and risk management practices?*

The third area addressed in this study of governance and risk management was to focus on what these organizations are doing to increase the comprehension and proficiencies in risk management at the board level and otherwise throughout the enterprise.

*A. To what extent is there formal risk management education at the board level?* In respect of the formal risk management education of board members, a majority of respondents have engaged in such, but a substantial minority (37 percent) have not held any formal educational programs for their board:

**Table 1.25**

HAS YOUR RISK MANAGEMENT ORGANIZATION HELD AN EDUCATIONAL SESSION FOR BOARD MEMBERS?		Response (%)	Response Count
Yes		63.0	29
No		37.0	17

One member of multiple boards made an important distinction in respect of how well supported the board is in the area of risk management. They noted that board risk committees do not commonly have outside expert

advisors available in the area of risk management to counsel committee members, while other board committees (such as compensation, audit) do regularly avail themselves of such outside experts as a part of their deliberations. This is, among other things, probably a reflection of the scarcity of independent professionals with sufficient risk industry experience, education and/or seniority, to meet this potential need.

## How Boards are Increasing Their Proficiency

These notes come from comments made by our interviewees:

- Often the board will arrange for practitioners from the firm to come to a meeting to discuss their specific product or their work.
- Working with the communications group on how they can transmit more risk management knowledge to employees.
- Each May is dedicated to an education-only session, with the agenda set by the audit and finance committees.
- New board members get a rigorous one-day or two half-day seminars that are packed with information.
- Quarterly, the risk team will focus on one specific risk issue and study it in great detail.
- They actively seek out board members from other companies, across different industries, and ask them about how they manage risk.

*B. To what extent is there formal risk management education at the employee level?* Another common indicator of governance activity is whether or not the firm provides ongoing education and training to all employees on the role of governance in the corporation. In respect of the specific area of risk management, just 13 percent of respondents “strongly agreed” that their regular training program for new employees included a focus on the risk management policy. An equal percentage “strongly agreed” that their employees are regularly updated about awareness of the risk management policy. Overall, only slightly more than half of the respondents “agreed” or “strongly agreed” that such a training program existed, which suggests there remains a significant gap in this element of good governance. (Note that this survey did not ask whether there was an ongoing training initiative for risk management employees alone, or whether other broad governance training programs existed. But we would assume that the risk management policy would be included in any such broad governance training and would thus have been noted by respondents.)

Our aforementioned concern that an awareness of risk policy may not be as high as believed is underscored further by noting that only slightly over half of the respondents indicate that they have a regular training program about risk management policies for new employees, even for these large – and presumably risk-sensitive – firms.

**Table 1.26**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
We have a regular training program for new employees that includes a focus on the risk management policy	13.3% (6)	37.8% (17)	13.3% (6)	28.9% (13)	6.7% (3)	45

Further, while a majority of the same firms say that they regularly update employees about the risk management policy, fully 21 percent – or more than 1 in 5 – indicate that their firm does not regularly update employees on risk policies.

**Table 1.27**

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Response Count
We regularly update our employees' awareness of the risk management policy	13.6% (6)	40.9% (18)	25.0% (11)	18.2% (8)	2.3% (1)	44

*C. To what extent does your company use external validation and benchmarking of governance processes?* A further inquiry into respondents' practices in implementing risk management is the use of outside reference sources to measure and critique the risk management systems employed by

the subject organization. Such a practice can provide a benchmarking of the effort and awareness of ongoing developments in the broader risk management industry.

In fact, we found that fewer than half of all respondents report using external consultants to provide them with benchmarking data.

**Table 1.28**

DO YOU USE AN OUTSIDE CONSULTANT TO BENCHMARK YOUR RISK MANAGEMENT ORGANIZATION PRACTICES AND INFRASTRUCTURE?		Response (%)	Response Count
Yes		45.7	21
No		54.3	25

Of those who do engage in external benchmarking via consultants, typically this was carried out every two years or so, with many commenting that benchmarking is done “as needed.”

**Table 1.29**

HOW OFTEN DO YOU USE AN EXTERNAL SOURCE FOR SUCH BENCHMARKING?		Response (%)	Response Count
Twice each year		0.0	0
Annually		33.3	4
Biannually (every two years)		66.7	8

### Assessing the Firm’s Risk Culture and Risk Awareness

One of our interviewees detailed a program that his firm has developed to assess the extent to which a risk-aware culture had permeated the firm. It is creatively based on a behavioral model that described a proactive risk culture in which people felt confident to report all mistakes or “bad news” to managers, who would then receive it affirmingly.

The core behaviors of this model are prevention, detection, recovery, and continuous improvement, which we note are highly aligned with the new work from OCEG in their Red Book 2.0 (see <http://www.oceg.org/view/foundation>). Together with key context influencers of role clarity, training, accountability and an encouraging environment, they define the status of the firm's risk culture.

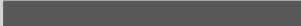

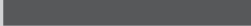

This firm uses their annual employee survey, which they report has an 84 percent participation rate, to ask 10 Risk Culture Index questions (spread throughout the survey) that focus on risk management behaviors.

The results from the survey are used to calculate a Risk Culture Score for all teams and business units within the company where there are more than 15 employees. The results are transparent to all managers and the performance assessment and annual bonus of each manager is partly dependent upon the risk culture score that their group achieves.

This company began their surveys in 2003 and has now rolled them out globally.

Of those firms who do not use consultants, most rely on industry reports and studies to provide them with guidance as an alternative source for information, with more than half relying on regulators to provide this service.

**Table 1.30**

PLEASE IDENTIFY ANY OF THE SOURCES BELOW THAT YOU USE FOR EXTERNAL BENCHMARKING:		Response (%)	Response Count
Industry reports and studies		89.2	33
Internal Audit		32.4	12
Regulators		54.1	20
Internal innovation and reporting		43.2	16

## Rating Agencies are Helping Some Firms

From one respondent: “We actually use various external sources including membership in the CRO Forum, Standard & Poor’s ERM rating, external consultants [and] membership of [various industry] bodies to monitor the performance of our Risk Function.”

The emergence of rating agency standards for ERM was also mentioned by another respondent.

In 2005, Standard & Poor’s began to include ERM in their rating evaluations for financial institutions and insurance companies. It has made an evaluation on two key types of information: the degree to which a firm has comprehensive mastery of the risks that it faces, and the extent to which the firm’s management optimizes revenue for the risk it is willing and able to take. In some cases, S&P asserts that its confidence in management’s ability to control risk taking allows them to conclude that a firm could absorb an apparently high level of potential risk exposure, and still qualify for high ratings. Conversely, firms with relatively low prima facie risk exposure, but with a weak ability to control risk, might receive lower ratings. S&P announced a plan to expand ERM ratings to the non-financial sector in 2008.

## How Do the “Smaller” Companies Compare to the Larger Companies?

Fifteen of the responses received were from firms that indicated they were not in the top 25 percent of firms in their industry. The substantial majority of the firms in this category (80 percent) report involvement in banking. We compare their responses on a several significant survey findings to those of the large firms:

- 43 percent (vs. 31 percent for the larger organizations) have a single board member responsible for being familiar with the risk management organization.
- 60 percent (vs. 37 percent) of these companies have an RMO that reports directly to the board.
- 93 percent (vs. 82 percent) have a chief risk officer or enterprise-wide risk officer.
- 87 percent (vs. 90 percent) have a risk policy.

- 77 percent (vs. 80 percent) agree that risk policy is well understood.
- 80 percent (vs. 76 percent) have a regular or other briefing for the entire board of directors.
- 92 percent (vs. 76 percent) believe their board is sufficiently skilled to understand the risk management organization and its reports.

It is interesting to note that on many of the study measures of risk management and governance organizational integration, the those firms in the survey sample that were either average in size or smaller than average appear to be more advanced than the larger firms in terms of the implementation of risk management within the governance structure. This may be a reflection of the complexity faced by the larger firms, or the fact that smaller companies have the ability to focus on organizational needs and to execute their plans more effectively. This is also probably a reflection of the sample bias. As noted, the firms invited to be participants in the survey were ones known to have risk management already in existence, and we believe it is not appropriate to extrapolate our findings to conclude that smaller firms are better than larger firms at risk management.

## Conclusion

Our survey responses and one-on-one interviews make it clear that the large companies who participated in our survey, many of them global leaders in their field, have rapidly advanced the effectiveness of the interaction between the board of directors and the risk management organizations over the past few years.

As various public and private bodies continue to develop and recommend interesting and innovative practices around the issue of governance it will be the actual implementations that determine what the standard will be in terms of shareholder expectations. The impact and importance of actual implementations may even extend to regulators as well if Basel II – Pillar I and Pillar III practices are emulated.

We found in the survey data that risk management is placed very high in the executive hierarchy of responding organizations. Most have risk policies in place and have RMOs who report, either directly or indirectly, to the board. There may be more confidence than is warranted that risk policies are understood throughout the firm since the education programs around such policies for new and existing employees appear to leave room for improvement.

Firms are pursuing risk management and governance for the purposes of competitive advantage, control, loss avoidance, and regulatory compliance. Often the same firm will be pursuing several such goals simultaneously.

There are multiple models for the assignment of board committee risk oversight. The most popular choice is a company's audit committee, but dedicated risk committees or executive (or management) committees are also popular. However, there are many other variations, including some dual assignments for this very important governance decision. A growing minority of firms have a single board member with responsibility for being familiar with the risk management organization of the firm. This is a highly challenging accountability, given that sufficiently skilled outside resources to support committee or individual oversight of the risk management organization are relatively scarce.

Most firms represented in our survey have held educational sessions for their boards, but a substantial percentage has not. Less than half of our respondents reported the use of outside consultants to help them to benchmark their internal practices. Rather, much reliance is placed upon a review of industry publications and studies, input from regulators and an emerging use of rating agency ERM reviews.

In the survey we identified several gaps between the current practices and those considered to be good principles of corporate governance. We especially note the need for further development of risk education and risk awareness at both board level and across the corporation in order to achieve the successful implementation of risk management with the overall governance structure. It can be concluded that further study of the means for effective communication of the corporate risk appetite, risk policy, and risk data/reporting expectations is warranted to ensure that firms are creating the kind of effective culture that their boards are increasingly seeking to foster.

## Appendix

In this section we provide a little more background on two matters of importance to the effectiveness of board oversight and its relationship to the risk management organization.

### The Influence of Authority and the Responsibility of the Board<sup>17</sup>

Within the world of organizational behavior, it is critical to have an understanding of how authority figures and authority structures influence corporate behavior. Research shows that of all modes of influence, authority is the one that chiefly distinguishes how people behave inside an organization from how they might behave as individuals outside of an organization. Employees, who are subject to the hierarchy, accept that those higher up the authority structure give commands and directions that are thought to specify what actions they should take to fulfill the plans of the organization. These directions, or policies, are often communicated in an incomplete manner.

Typically, middle level managers or line employees within a company will not know which of the choices that are available to them best maximize the organization's objectives. For example, should a company increase its rate of production and accept the likely increase in production errors that come with that change, or is it more important to meet the customers' expectations of quality? If the order to increase production comes from higher up the hierarchy, it will be assumed that it is based on expertise and knowledge. Most employees will treat authority within an organization as being legitimate, expert and a requirement of a complex structure that relies on a coordination of tasks.

The most critical breakdown in the effective implementation of top-level objectives and policies is the belief by superiors that their subordinates have sufficient knowledge and sufficient understanding of the intent of the orders they receive. Often this means that the higher-ups will not even be contemplating the possibility that their instructions have not been understood fully.

Within most firms risk management policies, corporate codes of conduct, and corporate procedures are already in place. However, these companies may well fall into the same trap. Just because these policies exist and have been established by the board or other top-level entities within the corporate hierarchy, does not mean they are understood fully. There is ample evidence in psychological literature that overconfidence that these policies are well understood is the norm.

If there is incomplete communication, a board may have an unwarranted belief that its governance structure is effective. Further, if those

lower down the hierarchy think that the board's failure to fully communicate their intent, or to effectively educate on their intent is a sign of their attitude toward such policies, the policies will have little effect and may, in fact, lead to behavior that runs counter to the intent of the policy.

#### Adherence to Commonly Found Governance Principles

In the preceding pages, we referenced several "common" governance principles. We draw the readers' attention to the PRMIA Governance Principles.<sup>18</sup> In 2004, an esteemed Blue Ribbon Advisory panel of the Professional Risk Managers' International Association (PRMIA) reviewed a number of existing best practice governance documents with the intent of identifying common principles that could be found in most, if not all. The objective of their exercise was to establish a minimum set of principles which should rightly be expected to be adhered to at all public companies.

From this study came the seven key PRMIA Governance Principles:

- Principle One: Sufficiency of Key Competencies
- Principle Two: Sufficiency of Resources and Process
- Principle Three: Independence of Key Parties
- Principle Four: Clear Accountability
- Principle Five: Ongoing Education and Discernment
- Principle Six: Disclosure and Transparency
- Principle Seven: External Validation

PRMIA uses these principles to develop applications to the board as well as to the organization as a whole. Some highlights from this include:

Boards and Audit Committees Must:

- Be effectively aware of the business structure and environment in which the corporation operates (sufficiency of key competencies, sufficiency of resources and process, ongoing education and discernment)

- Be composed in a manner such that sufficient independence and expertise exist to competently evaluate the business structure and environment in which the corporation operates (independence of key parties, sufficiency of key competencies, disclosure and transparency)
- Clearly articulate the corporate risk appetite to senior management (clear accountability, disclosure and transparency, ongoing education and discernment)
- Thoroughly review compensation plans of potentially “highly compensated positions” for consistency with corporate risk appetite, competitive market conditions and fiduciary responsibility to shareholders (independence of key parties, disclosure and transparency, ongoing education and discernment)
- Have a single member formally given responsibility for understanding and reporting the effectiveness of the corporation’s risk management infrastructure (sufficiency of key competencies, sufficiency of resources and process, clear accountability, disclosure and transparency)
- Continually review the application of standards of corporate governance to the risk management infrastructure, financial accounting and reporting infrastructure and the organization as a whole (clear accountability, ongoing education and discernment, external validation)
- Be fully accountable to shareholders through equitable voting rights (sufficiency of resources and process, clear accountability)

**The Risk Management Infrastructure Must:**

- Be independently staffed and report to an executive committee (operating committee) level employee who is not a business unit leader (Independence of key parties, clear accountability)
- Be of sufficient funding, intellectual and technological capacity to adequately understand and communicate the risks presented by the business structure and environment (Sufficiency of key competencies, sufficiency of resources and process, disclosure and transparency)

- To the extent possible, avoid silos of control and oversight (sufficiency of resources and process, clear accountability)
- Have a budget that is established by a subset of the executive committee or board, excluding the influence of individual business-unit leaders (independence of key parties, sufficiency of resources and process)
- Provide a clear escalation policy for the employees of the organization as a whole to escalate matters of concern without the threat of inappropriately adverse impact (independence of key parties, sufficiency of resources and process)
- Actively provide ongoing professional development for risk management staff and require them to be committed to standards of best practice, conduct and ethics in their work (sufficiency of key competencies, sufficiency of resources and process, ongoing education and discernment)
- Provide general corporate governance training for employees of the organization as a whole (sufficiency of resources and process, ongoing education and discernment)

#### Financial Accounting and Reporting Infrastructure Must:

- Accurately represent the corporation's current and known financial condition in a timely manner (disclosure and transparency)
- Only use off-balance sheet transactions which have a legitimate economic, tax, risk transfer or risk mitigating purpose (clear accountability, disclosure and transparency)
- Provide a detailed description of the risk management infrastructure in the corporation's annual report to shareholders (disclosure and transparency, ongoing education and discernment)
- Provide an auditable annual statement of compliance with the board's publicly stated standards of corporate governance to the board and audit committee (disclosure and transparency, ongoing education and discernment, external validation)

#### The Organization as a Whole Must:

- Provide ongoing education and training to all employees on the role of risk management and corporate governance in the corporation (ongoing education and discernment)
- Provide an environment in which an escalation policy can be effective (disclosure and transparency)
- Commit itself to actual enforcement of corporate governance polices (clear accountability) Commit itself to full compliance with local laws, regulations and customs, to the extent that such customs do not conflict with local laws and regulations (ongoing education and discernment)
- Publish an external auditor's opinion that the corporation is in compliance with the board's publicly stated standards of corporate governance (disclosure and transparency, external validation)

### Notes

- 1 See <http://www.ctwinvestmentgroup.com/index.php?id=58>.
- 2 See <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/21/AR2007112102335.html>.
- 3 See [http://www.businessweek.com/magazine/content/08\\_09/b4073030425608.htm?chan=top+news\\_top+news+index\\_businessweek+exclusives](http://www.businessweek.com/magazine/content/08_09/b4073030425608.htm?chan=top+news_top+news+index_businessweek+exclusives).
- 4 See [http://www.bloomberg.com/apps/news?pid=20601087&sid=anPpji\\_PBsF8&refer=home](http://www.bloomberg.com/apps/news?pid=20601087&sid=anPpji_PBsF8&refer=home).
- 5 See <http://www.reuters.com/article/bondsNews/idUSWNAS277720071116>.
- 6 Many discussions of a director's obligations, duties and challenges are available. For example, see John L. Colley 2003. *Corporate Governance*. New York: McGraw-Hill Professional.
- 7 These duties are actually based upon laws of the state where the corporation is chartered; however there are many approximate statements of the duties in the US generally. See, for example, American Law Institute. 1992. *Principles of Corporate Governance: Analysis and Recommendations*.
- 8 Financial reasons for managers to manage risk have been described by various authors' literature since the 1980s. A textbook discussion is found in Mark Grinblatt and Sheridan Teitman. 2001. *Financial Markets and Corporate Strategy*. Boston: Irwin/McGraw Hill.
- 9 Agency theory and the need to monitor the alignment of shareholder/manager interests have been described by many authors. See, for example, E. Fama and

- M. Jensen. 1983. Separation of ownership and control. *Journal of Law and Economics*, 26 (June): 301–25.
- 10 Directors' duties are widely described. See, for example, Dennis J. Block, Nancy E. Barton, Stephen A. Radin. 1998. *The Business Judgment Rule: Fiduciary Duties of Corporate Directors*, 5th edn. New York: Aspen Law & Business.
  - 11 These board obligations for sound controls have been discussed more in relation to implementing accounting and audit functions than risk management, per se. However, the arguments are generally applicable. See, for example, J. Cohen, G. Krishnamoorthy and A. Wright. 2002. Corporate governance and the audit process. *Contemporary Accounting Research*, 19(4) (Winter): 573.
  - 12 See <http://www.coso.org/>.
  - 13 See <http://www.oceg.org/Default.aspx>.
  - 14 James Lam. 2003. *Enterprise Risk Management: From Incentives to Controls*. Hoboken, NJ: Wiley.
  - 15 See <http://www.riskmanagement.com.au/>.
  - 16 See John Darley, David Messick and Tom Tyler. 2001. *Social Influences on Ethical Behavior in Organizations*. Mahwah, NJ: Lawrence Erlbaum Associates Publications.
  - 17 This is a summary of some key points made by John Darley in his essay "The Dynamics of Authority Influence in Organizations and the Unintended Action Consequences." In John Darley, David Messick and Tom Tyler. 2001. *Social Influences on Ethical Behavior in Organizations*. Mahwah, NJ: Lawrence Erlbaum Associates Publications.
  - 18 See [http://www.prmia.org/pdf/PRMIA\\_Governance\\_Principles.PDF](http://www.prmia.org/pdf/PRMIA_Governance_Principles.PDF).

