



Review **December 2010**

Risk Watch

Thought Leadership in Risk and Governance

Board Accountability for Risk Communication—Clear As Mud? [[Pages 2–5](#)]

Are We Missing the Big Ship? [[Pages 6–8](#)]

How Good Is Our Risk Management? [[Pages 9–12](#)]

Are Board Risk Committees a Fiduciary Expectation? [[Pages 13–17](#)]

Risk Management in the Public Sector [[Pages 18–20](#)]

Table of Contents

Preface	1
Board Accountability for Risk Communication—Clear As Mud?	2
Are We Missing the Big Ship?	6
How Good Is Our Risk Management?	9
Are Board Risk Committees a Fiduciary Expectation?	13
Risk Management in the Public Sector	18

ACKNOWLEDGEMENTS

The Conference Board of Canada would like to thank the authors for contributing their articles and for the teamwork involved in ensuring a seamless delivery of this publication.

Are Board Risk Committees a Fiduciary Expectation?

Businesses exist to take risk. Without the acceptance of this premise, there is no reason to deploy capital and no reason for a governance function to exist. The fiduciary governance of a business' strategy, and therefore the firm's risk taking, rests with the board of directors. Yet, with complex organizations, sufficiently meeting the fiduciary obligation of care—in which risk taking and risk management are embedded—may require a more specialized understanding of risk than can be managed effectively by the board as a whole.

UNDERSTANDING THE RISKS THAT MATTER

The single biggest risk that any organization faces is that it fails to anticipate what its customers' future needs will be. That risk is one clearly owned by the board as a whole as it focuses on the strategic plans of the organization.

But some important elements of risk may fall outside normal strategy discussions. Some negative risks, if realized, may be large enough to end the viability of even the most customer-prescient strategic plan. Further, more knowledgeable risk taking, which can improve the bottom

line, requires an understanding of both risk-taking capacity and the price of risk. These are almost certainly outside typical board strategy discussions.

Although a board audit committee may have defined accountability for the specialized knowledge of finance and the validity of financial reporting practices of the business, perhaps an additional scrutiny of risk may best be owned by a board's risk committee—which has an articulated focus on threats to the system (business), corporate resiliency, the effective use of risk capital, and communication regarding risk-taking capacity.

FORMATION OF RISK COMMITTEES OF THE BOARD

Nancy Foster, who served as executive vice-president and chief risk officer of CIT Group, Inc. until the end of 2009, said that her company's choice to initiate a board risk committee was primarily to deepen the board's participation in risk management. At CIT, the chief executive officer and lead director determined the composition of the committee and decided not to saddle the audit committee with the extra duties of a risk committee. This decision was made because the audit committee's agendas were regularly quite

Note on Sources

Unless otherwise noted, quoted text or opinions in this article are taken from conversations, online questionnaires, and e-mail exchanges between the author and the individuals named.

full, and the organization believed that more attention should be given to risk management.

CIT's present risk committee ("Risk Management Committee" is its official title) comprises three directors, all of whom are independent. The committee's charter clearly defines its areas of focus as specialized risks (market, credit, operational, reputational, and business continuity) and their processes for control.¹ It also highlights the need for coordination with the board-level audit committee and compensation committee, as each has a fiduciary responsibility for an area in which large and impactful risks have been realized at other organizations.

CIT's case is a special one in that its board risk management committee was formed as the financial crisis was emerging, and the company entered into bankruptcy late in 2009. It emerged from that bankruptcy in just 40 days² and subsequently reconstituted its board

of directors while keeping a board-level risk management committee in the governance structure. Since its re-emergence and re-listing on the NYSE in December 2009, the company's stock price has risen 50 per cent, compared with a rise in the S&P 500 index of around 10 per cent over the same period.³

But board-level risk committees are reserved not only for large financial institutions. Labor Finders International is a Florida-based, privately held industrial staffing company with more than 200 offices throughout the U.S. and more than 200,000 customers.⁴ According to Wayne Salen, the director of risk management, he and the CEO agreed that the board audit committee was not broad-based enough nor experienced enough in risk management to be able to adequately deal with risk on an enterprise-wide approach.

Julie Garland McLellan, who sits on a portfolio of boards in Australia, noted similar concerns among some of her boards, saying: ". . . some of my companies decided to start risk committees to oversee their risk system or to reduce the workload on the audit committee." She continued: "Each company made the decision based on consideration of the current operating conditions, the future strategy and its likely risks, the current skills in board and management, and the workload of existing board committees."

In other cases, a board risk committee has been considered but decided against. Boston-based Web Industries, Inc. provides contract manufacturing services (including supply chain management solutions) for flexible materials and serves many industries—medical, composites, consumer products, photovoltaic films, and more.⁵ Board member Stephen

Ringlee said: "We have considered a risk committee to offload some of the charter of the existing audit committee, but concluded that we are better served by a different approach that separates out control, compliance, and business risks, and manages them separately." He continued: "The audit committee will continue to focus on the first two categories since it has a process and expertise for identifying and managing both. The board as a whole will manage the third category through a rubric yet to be developed, which will constitute a checklist of questions and probes to be applied to a variety of business decisions and situations during the course of each board discussion, and which will be designed to help illuminate risk as an element in our decisions."

In commenting further on why the audit committee was not chosen to focus on risk governance, Ringlee noted that the audit committee has specialized expertise in control and compliance and has developed agendas and a history of probing in just these areas. "Business risks are much broader and belong at the board table using a workable approach to inform every business decision with concerns for and structures to help analyze risk," he said.

Leslie Thompson, who serves as a director of the Ontario Municipal Employees Retirement System and of the Deposit Insurance Corporation of Ontario, believes that the decision on whether to form a specialized risk committee is not always clear and should involve consideration of the nature of the organization's activities or business, the maturity and robustness of the organization's existing risk management practices, and the nature of their stakeholders. "A qualified risk committee,"

she said, "can give external stakeholders—such as significant investors, regulators, and rating agencies—confidence in an organization's management of uncertainty." Further, she argued, ". . . a risk committee can put pressure on the C-suite to improve their practices and suggest changes that would not be articulated at a regular board meeting because of timing, board composition, or a concern that it was 'in the weeds.'"

REQUIREMENTS OF A BOARD-LEVEL RISK COMMITTEE

According to a report released in August 2010 by the global 100 law firm Nixon Peabody LLP, one of the duties of a Delaware (U.S.) corporation is to provide oversight of the organization's risk management, including a good-faith attempt to oversee and monitor reporting and information systems designed to identify risks.⁶ Some of the duties of a board risk committee, which Nixon Peabody identifies as being possible, include:

- determining important operational risks and potentially catastrophic risks;
- making recommendations on the risk-taking capacity of the organization;
- overseeing enterprise-wide risk management practices;
- establishing quantitative and qualitative risk and reward goals, and monitoring key risks;
- ensuring that official reports properly disclose risks and risk factors; and
- reviewing communication flows to ensure a proper flow of information related to risks.

The law firm notes that the responsibility for the oversight of risk remains with the board as a whole, but that a risk committee could assist the board in exercising those duties.

Sometimes, fiduciary requirements are defined by explicit law, such as the U.S.-based Dodd-Frank Act. Other times, they arise via wide adoption of best practice principles, thus becoming the definition of “reasonable” when evaluating the fulfilment of the duty of care required of board members in the U.S. and Canada.

In 2007, The Conference Board, Inc. reported on emerging governance practices in enterprise risk management. The Board stated that: “While the board as a whole has an oversight role, it is unrealistic to believe that all directors may be equally involved in an effort that is highly specialized and time-consuming.”⁷ The report suggested that audit committees can act as a catalyst for enterprise risk management program development, but that the board should be sensitive to the issue of possibly overloading the agenda of the audit committee. “Boards,” it continued, “should consider the assignment of certain risk oversight functions to other committees (or even the formation of a dedicated risk committee).”

In its *Principles of Good Governance*, the Professional Risk Managers’ International Association (PRMIA), representing more than 70,000 members in 200 countries, specifically refers to audit committees and risk committees, as well as the board as a whole, as having obligations for risk governance.⁸ Among the obligations of boards, and these committees, are responsibility for knowledge of the risk management infrastructure, and the definition and communication of a risk appetite; setting compensation programs that adhere to the risk appetite and fiduciary responsibilities to shareholders; and “[delegating]—to one of their number—formal responsibility for understanding, in detail, the risk management infrastructure

of the organization, and for reporting regularly to the board of directors/committee on the effectiveness of that infrastructure.”

These two important groups seem to be setting the stage for a strong argument that board-level risk committees are a de facto standard of good governance, and may be interpreted as an obligation in the fulfilment of the fiduciary duty of care.

THE DECISION TO ESTABLISH A RISK COMMITTEE OF THE BOARD

In a recent session with the board of a well-established, non-profit organization, I put forward a list of questions that I felt would help the board address their fiduciary role and assess whether they understood their risks, both positive and negative. (See box “Questions for the Board” on the next page.) If all of these questions can be answered by the board as a whole—without sacrifice of significant time to be spent on other fiduciary obligations, and with sufficient expertise—then the establishment of a risk committee of the board may not be needed. The questions are applicable across the for-profit and non-profit sectors.

CHALLENGES

It is clear that one of the biggest challenges faced by those who have decided to establish a board-level risk committee is the provision of sufficient technical talent. The modern practice of risk management began roughly 25 years ago. Senior executives with sufficient overall business experience and requisite risk management experience are rare.

Wayne Salen of Labor Finders International said: “Training was the only challenge we ran into due to some perspectives out there that still saw risk as being only incident/hazard/event-based as opposed to our new holistic approach.”

Associations like PRMIA have partnered with leading business schools such as Columbia Business School and Kellogg Graduate School of Management, among others, to offer extended and compact versions of a “Complete Course in Risk Management” that seeks to address such needs. As well, they are developing more board-specific educational programs.⁹ The Directors College, a joint venture of The Conference Board of Canada and McMaster University, is likewise active in the development of these critical skills among directors.¹⁰

Another way to address this challenge was noted by Paul Goncharoff, who served until May 2009 as an independent director for Bank24.ru in Russia. He said that their risk committee involved fewer board members than most committees and that “in order to refine perspective, more middle-level ‘frontline’ employees participate than in any other committee, which seems to [have worked] well so far.”

Another common challenge cited in discussions with directors who have created risk committees is the establishment of a proper framework for engaging the risk management infrastructure of the organization and its risk policies and procedures. Audit committees have long histories with such frameworks, and the newness of risk committees—as well as the risk management practice—makes this more challenging for organizations interested in appropriately fulfilling their duty of care.

Questions for the Board

QUESTIONS ON THE APPETITE FOR RISK

- ◆ What amount of loss could you sustain, and not drain your reserves/capital?
 - How long would it take to recover via “normal” business operations?
- ◆ What kinds of things would you never tolerate or never want to read about in the newspaper?
- ◆ What are your sources of revenue and what could threaten them?
 - If any one loss would be big enough to disrupt services, what is your contingency plan?
- ◆ What would you like to do but are not doing because of some fear?
 - What opportunities are you missing by not taking action?
 - What could you do with your organization if a new idea proves to be successful?

GENERAL DUTY-OF-CARE QUESTIONS RELATED TO RISK MANAGEMENT

- ◆ Have you developed a disaster recovery plan?
 - If so, do you validate that it has been tested at least annually?
- ◆ Have you created a “book of risks”?
- ◆ How do you measure your risks and know that they are of an appropriate size and not increasing?
- ◆ Do you ever meet without the chief executive present?
- ◆ Do you have a way for concerns to be escalated to the board without staff interference or interpretation?
- ◆ Does your administrative team track risk events, actions, and outcomes for a future review by the board?
- ◆ How do you validate that the board’s vision and policies are understood by all employees, and by volunteers who work at a non-profit organization?
- ◆ What are the specific measures and targets that you use to evaluate your progress toward long-term and short-term goals and are they consistent with your risk appetite?
- ◆ What is the risk of not taking a risk in pursuit of new goals or new areas of service?
- ◆ What are the ethical and cultural priorities that attract stakeholders to your organization?
- ◆ Do you have a way to gather input from stakeholders directly?
- ◆ How do you monitor changes in the external environment?
- ◆ Do you regularly assess, in a repetitive and comparable manner, the satisfaction with your services that customers and external influencers have?
- ◆ How do you ensure that your employees are always growing in their risk management skills?

Source: David R. Koenig

internal counsel, external advisors, and benchmarking to existing charters at peer institutions.

JPMorgan Chase has adopted a very simple risk (policy) committee charter that notes its mission as being “responsible for oversight of the CEO’s and senior management’s responsibilities to assess and manage the corporation’s credit risk, market risk, interest rate risk, investment risk, liquidity risk, and reputational risk; and also responsible for review of the corporation’s fiduciary and asset management activities.”¹¹ This policy clearly delineates the oversight role of the board from the management responsibilities of senior executives, which is a helpful reminder of their important but distinct accountabilities.

Compare and contrast the JPMorgan Chase charter with Northern Trust’s (business) risk committee charter. The latter is five pages in length and contains unfortunate “wiggle” language that seems to disown responsibility for validation of management’s reports to the risk committee: “Each member of the Committee shall be entitled to rely in good faith on (i) the integrity of those persons and organizations within and outside Northern Trust from which he or she receives information, and (ii) the accuracy of the information provided to the Committee by such persons or organizations absent actual knowledge to the contrary (which shall be promptly reported to the Board).”¹²

The Internet Corporation for Assigned Names and Numbers (ICANN)—the governors of Internet names and numbers—also has a board risk committee. Its charter is simple and straightforward.¹³ As you might imagine, its focus is on

At Web Industries, Inc., the board is planning to “draft a ‘risk rubric’” to help board members highlight, assess, and better understand the dimensions of business risk among all their decisions, according to Steve Ringlee. He continued: “This will be done by board members and management; the work load is yet to be determined.”

CHARTERS AND GUIDANCE

Risk committee charters attempt to set forth the boundaries of the committee’s responsibilities, illuminate the need for collaboration with other committees, and establish broad responsibility for risk oversight for the board as a whole. The charters vary in complexity and commitment, with their construct guided by

non-financial risks, including oversight of risk management for the organization as a whole and oversight of operational activities. Carefully balancing the positive and negative domains of risk, the committee is concerned about general operational risks, the effectiveness of the technology utilized by ICANN, and changes in the business environment that may be material to ICANN operations, among other risks.

“Assessment of the integrity of the risk management function,” as is directed in the risk committee charter of Credit Suisse, is probably the largest challenge facing most boards. Given the limited talent pool of those who have both sufficient practical executive experience in risk management and the strategic business planning skills required as a general board member, it may not yet be reasonable to imagine all boards of publicly traded companies being able to fulfill this directive completely. As one method to fulfill the obligation of reasonable care, the board risk committee can review, in detail, the documentation of discussions that management has about hypothetical business and risk scenarios. Or the committee may engage external advisors to validate certain risk calculations that form the foundation of risk capital allocations. It is important, though, that such sampling is truly random and that management is able to produce required access or documentation without significant delay.

CONCLUSION

Board fiduciary responsibility includes a duty of care that it must reasonably fulfill. That care is both in the development of strategy and the understanding of risks taken in pursuit of strategic goals. Some negative risks associated

with operations and the pursuit of goals may be large enough, if realized, to impair the organization’s ability to pursue any of its goals. At the same time, a better understanding of risk can allow organizations to more effectively take risks and achieve better returns for shareholders.

In most complex organizations, a board-level understanding of both risk-taking capacity and the pricing of risks is going to be achievable only through the establishment of a separately accountable board risk committee.



David R. Koenig
Chief Executive Officer
The Governance Fund
Advisors, LLC

David R. Koenig is a 25-year veteran of the financial services industry. His current employer is an investment management company focused on discovering value in well-governed companies and the under-appreciated risk in those that are not. He is the author of Governance, the working title of a book to be published by John Wiley & Sons in 2011. Mr. Koenig served as Chair, Board of Directors of the Professional Risk Managers’ International Association, and led the development of three risk management programs. He was recently awarded an M-Prize (Honorable Mention) by the Management Innovation eXchange (MIX) for his concept of Risk Capital as Commons: Distributive and Networked Governance. He can be reached at david.koenig@thegovfund.com.

- 1 CIT Group Inc., *Charter of the Risk Management Committee of the Board of Directors*. Amended January 10, 2010. www.cit.com/wcmprod/groups/content/@wcm/@cit/@corporate-governance/documents/information/s4005754.pdf.
- 2 CIT Group Inc., *The History of CIT*. www.cit.com/wcmprod/groups/content/@wcm/@cit/@media/documents/fact-sheets/cit-centennial-121009.pdf.
- 3 As of November 10, 2010.
- 4 LinkedIn, “Labor Finders.” www.linkedin.com/company/46819?trk=null.
- 5 LinkedIn, “Web Industries.” www.linkedin.com/company/web-industries?goback=.cps_1289852601578_1&trk=co_search_results.
- 6 John C. Partigan and Daniel McAvoy, “The Role and Construction of Risk Committees,” *Corporate Responsibility Alert* (August 11, 2010). www.nixonpeabody.com/linked_media/publications/Corporate_%20Responsibility_Alert_08_11_2010.pdf.
- 7 Matteo Tonello, *Emerging Government Practices in Enterprise Risk Management* (New York: The Conference Board, Inc., February 2007). www.conferenceboard.ca/documents.aspx?did=1914.
- 8 Professional Risk Managers’ International Association, *Principles of Good Governance* (Wilmington: PRMIA, September 2009). www.prmia.org/pdf/Case_Studies/PRMIA_Principles_of_Good_Governance_4_2.pdf.
- 9 Professional Risk Managers’ International Association, “A Complete Course in Risk Management.” www.prmia.org/Weblogs/General/PRMIA_docs/CompleteCourseFlyerNov10.pdf.
- 10 The Directors College. <http://thedirectorscollege.com/>.
- 11 JPMorgan Chase & Co., “Risk Policy Committee Charter.” www.jpmorganchase.com/corporate/About-JPMC/risk-committee-charter.htm.
- 12 Northern Trust Corporation, “Business Risk Committee Charter.” www-ac.northerntrust.com/content/media/attachment/data/compliance/0611/document/CGBusinessRiskCommitteeCharter.pdf.
- 13 Internet Corporation for Assigned Names and Numbers, “Risk Committee Charter.” www.icann.org/en/committees/risk/charter.htm.

About The Conference Board of Canada

We are:

- The foremost independent, not-for-profit, applied research organization in Canada.
- Objective and non-partisan. We do not lobby for specific interests.
- Funded exclusively through the fees we charge for services to the private and public sectors.
- Experts in running conferences but also at conducting, publishing, and disseminating research; helping people network; developing individual leadership skills; and building organizational capacity.
- Specialists in economic trends, as well as organizational performance and public policy issues.
- Not a government department or agency, although we are often hired to provide services for all levels of government.
- Independent from, but affiliated with, The Conference Board, Inc. of New York, which serves nearly 2,000 companies in 60 nations and has offices in Brussels and Hong Kong.

Publication 11-055
E-copy: \$170

The Conference Board of Canada
Insights You Can Count On



255 Smyth Road, Ottawa ON K1H 8M7 Canada
Tel. 613-526-3280 • Fax 613-526-4857 • Inquiries 1-866-711-2262

