

Challenges and Changes Guidance for Boards on the Oversight of Risk

By Brian Ferguson, CA

Chair, Risk Management and Governance Board
Canadian Institute of Chartered Accountants

Risk has been described recently as “the ultimate four-letter word” and, for many boards, that appears to be the case. In the wake of the financial crisis, much has been said about the failure of corporate boards to properly oversee risk management. New regulations have been proposed in several jurisdictions to better address the board’s responsibility for risk.

What exactly is the appropriate role of the board in corporate risk management?

What exactly is the appropriate role of the board in corporate risk management? Boards cannot and should not be involved in day-to-day risk management; but directors should, through their oversight role, be able to satisfy themselves that

effective risk management processes are in place and implemented. The risk management system should allow management to bring to the board’s attention the company’s most

material risks and assist the board in understanding and evaluating how these risks interrelate, how they may affect the company and how they are being addressed by management.

In certain cases, boards must take a more active role in risk assessment, such as risks associated with leadership, since management cannot always be expected to objectively assess itself from a risk perspective.

Unlike other embedded responsibilities of boards and committees such as the oversight of financial reporting and disclosure, there are currently no standards for the oversight of risk and few authoritative sources upon which Canadian boards may rely.

Risk Oversight and Governance Board

To better reflect directors’ responsibility for the oversight of risk management, the Risk Management and Governance Board of the CICA, which I chair, has changed its name to the Risk **Oversight** and Governance Board.

To assist directors in fulfilling their responsibilities, we are currently developing a framework for risk oversight at the board level, authored by experienced corporate



director John Caldwell. Some of the building blocks of this framework are discussed below.

A Framework for Board Oversight of Risk

The board's role in the oversight of risk is similar in some ways to the role of the audit committee. The audit committee does not prepare financial statements or draft disclosures nor maintain the system of internal control. Rather, the audit committee bears the responsibility of overseeing the financial reporting and control processes. Similarly, boards are not expected to identify, analyze, mitigate and monitor enterprise risk. Rather, they oversee the risk management systems and processes and continuously review the related planning and outcomes. This oversight role should not be passive in nature nor should the board be excessively reliant on management.

Successful oversight of risk by the board requires confidence in management, access to relevant and reliable information and effective functioning of the board overall.

Boards should ensure that they have a clear understanding of their role when it comes to risk. They should also address the way in which they are organized to oversee risk management. This was recently identified by the National Association of Corporate Directors (NACD) in the U.S. in its Blue Ribbon Commission report on risk governance as a key principle to guide directors in their efforts to provide effective risk oversight.¹

There is not one right way to organize the board to oversee risk. In some organizations, responsibility for certain risks is assigned to committees such as audit or risk committees. In others, risk remains with the full board. However, some boards fail to assign responsibility at all.

Questions directors should consider include:

- Is responsibility for risk oversight clearly set out in the board's mandate?
- If responsibility for certain areas of risk is delegated to committees, are the terms of delegation clear and does the committee have the capability to oversee risk in its broadest form?

- Is sufficient time set aside to carry out risk oversight responsibilities?
- Do board agendas promote integration of risk issues with other agenda items such as strategy and finance?

Where responsibility for certain areas of risk is delegated to committees, it should be clear that the full board retains overall responsibility for risk as it affects the organization. Care should also be taken to ensure that the use of committees does not result in risks being considered in silos, missing the potential implications of interconnected risks.

Boards should ensure that responsibility for risk oversight is clear to investors, regulators and other stakeholders. The Securities and Exchange Commission (SEC) in the U.S. has proposed changes to proxy disclosures which would require a description in proxy statements of the board's role in risk management, on the basis that this disclosure should provide important information to investors about how the board perceives and manages the company's risks. The proposal states:

Given the role that risk and the adequacy of risk oversight have played in the recent market crisis, we believe it is important for investors to understand the board's, or board committee's role in this area. For example, how does the board implement and manage its risk management function, through the board as a whole or through a committee, such as the audit committee? Such disclosure might address questions such as whether the persons who oversee risk management report directly to the board as whole, to a committee, such as the audit committee, or to one of the other standing committees of the board; and whether and how the board, or board committee, monitors risk.²

The Board's Relationship with Management

Once the board is clear on its responsibility for risk oversight and the way it is organized to address that responsibility, directors should ensure that management shares the same understanding. The quality of the interaction between management and the board will have a major effect on the ability of the

¹ Report of the NACD Blue Ribbon Commission. *Risk Governance: Balancing Risk and Reward*. National Association of Corporate Directors, October 2009.

² SEC Release Nos. 33-9052; 34-60280; IC-28817; File No. S7-13-09 (July 10, 2009) at p. 35.

board to effectively oversee risk as well as the overall risk culture of the organization.

The NACD recommends in its report that boards work with management to understand and agree on the types and format of risk information the board requires. It is critical to encourage a dynamic and constructive risk dialogue between management and the board, including a willingness to challenge assumptions.

The recently released *Review of corporate governance in UK banks and other financial industry entities* (Walker report) speaks to the necessity of changing board culture in some cases so that “disciplined but rigorous challenge” on substantive issues such as strategic risk comes to be seen as the norm. The report describes an informal contract between directors and the CEO “under which the former are expected to be challenging”.³ However, once a board decision is reached, the CEO should have the full support of the board in implementing it.

Questions for directors to consider include:

- Does the board receive adequate, timely and relevant information on risk?
- Does the board have access to outside experts when necessary to advise on risk identification and assessment?
- Does the board too readily accept management’s assessment of risk, particularly risks which management may be unable to assess objectively?

An effective board oversight process sets aside sufficient time at and between meetings for reflection and obtaining additional information. Each board meeting should include *in camera* sessions without management present.

Setting the Organization’s Risk Tolerance Policy

Appropriately balancing risk and reward is fundamental to any business.

Appropriately balancing risk and reward is fundamental to any business. However, risk tolerance varies among corporations depending upon factors such as size and maturity, capital structure, ownership, geographic concentration and other industry-specific characteristics.

Setting the organization’s risk tolerance policy is a key role of the board and is increasingly appearing in corporate governance regulations. Changes recently proposed to the UK Combined Code of Corporate Governance include a clear statement that the board is responsible for defining the company’s risk appetite and tolerance.⁴ In South Africa, the *King Report on Governance for South Africa* (King III), released in September of this year, recommends that boards set the levels of risk tolerance once a year.⁵

Risk tolerance should be related to how a corporation views adverse consequential exposure or potential damage. For example, early stage corporations may be willing to sustain considerable losses as they develop and bring new products to market. Mature corporations may set their risk tolerance thresholds at a defined level of underperformance. A corporation’s tolerance for risk will be influenced by its capacity to withstand adverse consequences.

One important element in sustaining a corporation is the strength of its capital structure. A well-financed corporation can withstand severe adversity, whereas a business with a weak balance sheet has little room for error or unexpected negative occurrences.

The organization’s capacity to take on and absorb risk should be periodically reviewed and quantified by the board. Once determined, the risk tolerance policy should be clearly communicated to management. New strategic initiatives, executive compensation and other policies should be assessed to be sure they are in line with the risk tolerance policy.

Board Leadership Required

A clear understanding of the role of the board, effective dialogue with management regarding risk and a clear and considered risk tolerance policy for the organization are the building blocks which will allow boards to effectively oversee risk. Further elements of the CICA’s framework for board oversight of risk will be discussed in future columns.

Mr. Ferguson and the Risk Oversight and Governance Board of the CICA can be reached at rogb@cica.ca
ROGB publications are available at www.rogb.ca

³ *A review of corporate governance in UK banks and other financial industry entities: Final recommendations.* David Walker, November 26, 2009 at paras 4.8

⁴ *Consultation on the Revised UK Corporate Governance Code.* Financial Reporting Council. December 2009

⁵ *King Code of Governance for South Africa 2009* s.4.2.1