



**RIMS Executive Report**  
*The Risk Perspective*

**An Evolving Model for Board Risk Governance**

# RIMS EXECUTIVE REPORT

## An Evolving Model for Board Risk Governance

By Carol Fox, John Bugalla and Kristina Narvaez

RIMS would like to acknowledge the following individuals for their support of this executive report:

### **Executive Director**

Mary Roth, RIMS Executive Director

### **RIMS ERM Committee Members**

Pete Fahrenthold, United Airlines

Ryan Egerdahl, Bonneville Power Authority

Grace Crickette, University of California

Radu Demian, University Hospitals Health System Inc.

Carol Fox, RIMS

John Hach, Lincoln Electric Co.

Jayashree Ishwar, Erie Insurance Group

Rupak Mazumdar, eHealth Ontario

Russell McGuire, Milliman Risk Advisory Services

Soubhagya Parija, Sterling Jewelers, Inc.

Nowell Seaman, University of Saskatchewan

Cristina Tate, Hewlett-Packard Company

Walt Williams, Lowe's Companies, Inc.

Drew Zavatsky, State of Washington

With the focus on board risk oversight being driven by external forces, what risk governance model is most appropriate for discharging a board's responsibilities for risk oversight? Perhaps more importantly, how does risk oversight align with the board's primary objectives?

In its 2009 Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies, the National Association of Corporate Directors (NACD) states that the "board's fiduciary objective is long-term value creation for the corporation; governance form and process should follow." So how do an organization's board structures and practices align with its risk oversight responsibilities, particularly as risk relates to the board's fiduciary objective for long-term value creation? With this question in mind, we will explore how a board's governance structure can influence how effectively risk is linked to the board's oversight of an organization's strategic and operational objectives.

The first question to consider is: Are board members satisfied that the risk reports they receive provide them with the information necessary to fulfill its risk oversight role? According to a 2009 study of 125 corporate directors in the United States, conducted by Miami University's Center of Business Excellence, just a little over half (54%) of the respondents reported that the risk information they receive is complete with respect to operational and strategic risks. Meanwhile, 92% of the corporate directors reported that more risk information pertaining to the strategic risks that might affect corporate strategy would be beneficial in the board's risk oversight role. These findings illustrate that the connection of risk management to the board's objective of long-term value creation has not yet been fully made.

### A TYPICAL RISK GOVERNANCE MODEL



Figure 1

As shown in Figure 1, the risk management function serves to enable the business risk owners and executive management to carry out their respective responsibilities for execution and the risk framework. Ultimate risk oversight responsibilities belong at the board level. This model of board risk oversight

is consistent across all enterprise risk management frameworks and standards. A 2010 Deloitte study of members of the Standard and Poor's 500 found that only 34% of the disclosures in the proxy filings of members of the S&P 500 noted whether risk oversight/management are aligned with the company's strategy and 58% of the disclosures noted that the audit committee is the primary committee responsible for risk.<sup>1</sup> These findings beg the question: Is the audit committee the right place for risk oversight, particularly as risk relates to the company's strategy? First, let's review the external forces driving risk governance oversight.

### RISK GOVERNANCE DRIVERS

According to a 2010 survey conducted by the Institutional Shareholders Services, investors and corporations alike are focusing on the importance of risk oversight.<sup>2</sup> In the survey, it was the most commonly cited topic of importance for issuers of public shares across all regions, clearly outstripping all other topics (with the one exception being executive compensation in North America). Two primary events have driven risk governance focus in the past 10 years: the financial scandals of 2002 and the financial crisis of 2008.



Figure 2

Figure 2 provides both a guide and timeline for the multiple major drivers that impact both risk governance and enterprise risk management for the foreseeable future. The first wave of governance drivers, particularly in the United States, was the result of the financial scandals in 2002:

- Sarbanes-Oxley led to rules for monitoring policies and procedures in the preparation of a company's financial and SEC reports.
- NYSE corporate governance rules required a company's audit committee

to discuss policies with respect to financial risk assessment and risk management.

- Rating agencies started to opine on ERM post-Enron and had been a primary driver of ERM implementations until the SEC Rule 33-9089 was issued in 2009.

While the financial crisis had a huge impact on the SEC's amending rule 33-9089, key legal cases have influenced board governance and its responsibilities for risk oversight. Delaware courts, for example, have held that the board's fiduciary duties include a duty to attempt in good faith to oversee and monitor the operation of the company's reporting or information systems designed to identify risks. The board is subject to liability for a failure in oversight where there is "a sustained or systematic failure to exercise oversight" or "an utter failure to attempt to ensure a reporting and information system has been implemented."<sup>3</sup> Companies are expected to implement appropriate risk reporting and monitoring systems and review these systems on a regular basis by shareholders, regulatory bodies and the courts.

This is not a new concept. The SEC has been requiring public companies to disclose their most significant risks relating to the ownership of the company's securities for some time in their annual and quarterly reports under the section entitled "Risk Factors." Taking this one step further, the SEC's amended rule 33-9089 adds requirements for proxy disclosures regarding a company's compensation policies and practices as they relate to the company's risk management practices, to the extent that risks arising from these compensation policies are reasonably likely to have a material adverse effect on the company. Companies are also required to disclose the extent of the board's role in risk oversight, such as administration of the oversight function.

The Dodd-Frank Wall Street Reform and Consumer Protection Act also has risk management implications. Because it touches so many different federal regulatory agencies, Dodd-Frank represents a paradigm shift in the U.S. financial regulatory environment. It is also the first statutory requirement for a risk committee. While some pundits argue that the Dodd-Frank Act went too far, others argue that it did not go far enough. Several additional bills have been introduced within the Congress for consideration, most notably the Shareholders Bill of Rights Act of 2009 in the Senate, and the Shareholder Empowerment Act of 2009 in the House. It is interesting to note that one of the provisions in these bills impose even stricter risk management requirements upon boards of directors, including one that requires all publicly traded companies to form a board level risk committee.

Additionally, HR. 3272 Corporate Governance Reform Act 2009 sponsored by Representative Keith Ellison (D-MN) proposes to amend the Securities and Exchange Act of 1934 to add requirements for board of directors committees regarding risk management and compensation policies, to require non-banking shareholder votes on executive compensation, and for other purposes. Under Section 3 of the bill, it requires that the composition of the board-level risk committee be limited to independent directors. The bill defines the term "risk management committee as a committee established by and amongst the board of directors of an issuer for the purpose of overseeing the risk management policies and procedures." Regardless of whether these bills are passed, it is evident that greater shareholder action pertaining to risk management can be expected.

## **RECENT DEVELOPMENTS IN THE UK AND CANADA**

In 2009, David Walker was directed by then Prime Minister Gordon Brown to undertake a review of corporate governance in UK banks and other financial industry entities due to the 2008 financial crisis. His final recommendations were published in November 2009 in what is known as "The Walker Report."<sup>4</sup> There are 39 recommendations contained in the report, five of which address risk governance:

- Requirement for and enhancing the remit of a board risk committee (23)
- Strengthening the role and independence of the chief risk officer (24)
- Ensuring that the board risk committee has appropriate access to external risk information (25)
- Due diligence by the board risk committee on significant acquisitions and disposals (26)
- Improving the annual reporting of risk management (27)

The Canadian Securities Administrators (CSA) recently proposed changes to the disclosure requirements pertaining to executive compensation and compensation committees. Under the proposals, companies would have to disclose, among other things, risks arising from compensation policies and practices that are likely to have a material adverse effect on the company. More generally, the CSA stated in its 2010 report on corporate governance disclosure that risk-management practices are under increased scrutiny, and regulators are monitoring this area closely.<sup>5</sup>

The Ontario Securities Commission (OSC) has announced a shareholder democracy initiative, which involves soliciting input from market participants on say-on-pay, majority voting and the overall effectiveness of the proxy voting system. Executive compensation and the work of compensation committees are under increased scrutiny, with new regulatory initiatives focusing on the relationship between compensation practices and risk management.<sup>6</sup>

## **HAVE THESE RISK GOVERNANCE DRIVERS BEEN SUCCESSFUL?**

One of the objectives of the SEC rule is to improve investor information and to assure investors that the board of a publicly traded company is involved with the oversight of risk – a key competency of the board. As the SEC rule was effective Feb 28, 2010, just before the primary financial reporting season, ermINSIGHTS, an enterprise risk management practices consulting firm, set out to measure the rule's impact by reviewing the proxy statements of the companies composing the Dow Jones Industrial Average. The study, conducted in late 2010, focused on the linkage of enterprise risk management with corporate governance by analyzing three aspects of the disclosures:

1. How often an organization noted whether a chief risk officer (CRO) function was in place
2. Measure the extent "enterprise risk management" or enterprise approach to risk management was specifically mentioned and
3. Examine how the board's role in risk oversight was being presented to stakeholders

SEC Concerns - "...disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company. This disclosure requirement gives companies the flexibility to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example.."<sup>7</sup>

The results are noted in Figure 3.

- 76% of proxy statements (form 14A) contained a section about board oversight of risk.
- 64% mentioned enterprise risk management or an enterprise approach
- 20% stated a chief risk officer (CRO) was in place

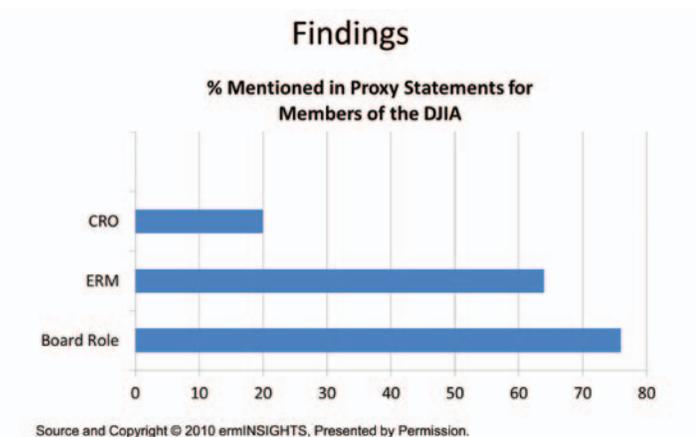


Figure 3

As many companies do not have a formal CRO, the study noted that in several cases a senior person undertook the risk officer responsibility, sometimes with the understanding that the role would rotate within the company. Due to the timing of ermINSIGHTS' study related to the company fiscal years, only 76% of the DJIA member proxy statements contained a section about board oversight. It is expected that following the full reporting cycle, there will be 100% compliance.

The SEC rule clearly raised risk management to the board agenda as never before. While the rule covers the disclosure of board risk oversight, the Dodd-Frank Act provides a structure for governance. Stand-alone risk committees are required at the board level at banks with consolidated assets of greater than \$10 billion, as well as certain non-bank financial companies supervised by the Board of Governors of the Federal Reserve Bank.

The Dodd-Frank Act is an important piece of legislation for U.S. companies and those doing business in the U.S. when one considers that:

1. Non-bank financial companies include insurance companies.
2. The law also applies to companies deemed systemically important to the U.S. economy.
3. Risk committees are required at the board level.
4. Risk committee responsibilities are for oversight – not management.

## DO THESE MAJOR DRIVERS SIGNAL A CHANGE IN BOARD GOVERNANCE STRUCTURE?

In the article entitled *The Growing Role of the Board in Risk Oversight*, the authors provide director-level perspective on whether risk oversight is better handled within an audit committee or a separate risk committee, "While risk oversight is a responsibility of all board directors and is handled in some companies at the full board level, it is typically owned by either the audit committee or a dedicated risk committee.<sup>8</sup> And while both the audit and risk committee approaches can both be effective, the nature of the organization and the kinds of risks the business faces can significantly influence which approach makes the most sense for a specific company."

The NACD Key Agreed Principle that "boards should explain to shareholders why the governance structures and practices it has developed are best suited to the company" also implies that no one governance structure fits all.<sup>9</sup> In fact, it seems to imply that organizations should customize their governance structure and practices based on the organization's individual character and needs.

Using the Institute of Internal Auditors and the NACD sample charters for audit committees and risk committees respectively as a benchmark against the actual charters, consulting firm ERM Strategies reviewed publically available board committee charters (see Figure 4) in the Fortune 100 compared against these sample charters.

### Dodd-Frank Risk Governance Directives

- Requires risk committees at certain non-bank financial companies and bank holding companies
- Responsible for the oversight of the enterprise-wide risk management practices including:
  - Certain number of independent directors (as determined by the Federal Reserve)
  - At least one risk management expert having experience in identifying, assessing and managing risk exposures of large, complex firms
- Does not mandate risk committees for all U.S. listed companies

## Organizations that formed Board Risk Committees in 2008 or after

Fortune 100		
<b>Insurers</b> <ul style="list-style-type: none"> <li>• AIG</li> <li>• Hartford</li> <li>• Travelers</li> </ul>	<b>Financial Institutions</b> <ul style="list-style-type: none"> <li>• Bank of America</li> <li>• Citigroup</li> <li>• Fannie Mae</li> <li>• Freddie Mac</li> <li>• Goldman Sachs</li> <li>• JP Morgan Chase</li> <li>• Morgan Stanley</li> <li>• TIAA-CREF</li> </ul>	<b>Auto Industry</b> <ul style="list-style-type: none"> <li>• General Motors</li> </ul>

Figure 4

The sample audit committee charters' Purpose section is focused on the validity of the organization's risk controls and the accuracy of its financial reporting. In contrast, the sample risk committee charter's Purpose section is focused on fulfilling its responsibilities for the risk management oversight described in the company's bylaws and corporate governance guidelines that is approved by the board.

The Duties and Responsibilities in the IIA Sample Audit Committee Charter require members to review the organization's financial statements, internal controls, external audit, compliance and reporting responsibilities.

The Duties and Responsibilities contained in the NACD Sample Risk Committee Charter require members to do one thing: monitor all enterprise risks. In doing so, the committee recognizes the responsibilities delegated to other committees by the board and understands that the other committees may emphasize specific risk monitoring through their respective activities. The members are expected to:

- Discuss the company's major risk exposures and the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies.
- Review all business units and consider risks that may affect the entire company's viability and the steps taken by management to manage these risks within an acceptable tolerance level.

The NACD's model sample proposes a single purpose risk committee, which would keep risk as a higher priority given the extensive commitments already required by audit committee members just to fulfill traditional audit committee tasks. However, some boards might consider a single purpose to be too narrow and possibly lead to a governance separation between risks and controls. ERM Strategies took a closer look at the General Motors (GM) governance model to determine how the automotive giant approached this issue.

### THE GENERAL MOTORS RISK GOVERNANCE MODEL

Prior to August 3, 2010, GM had an Investment Fund Committee, which was dissolved and ultimately replaced with a Finance and Risk Committee on December 7, 2010.<sup>10</sup> This new committee focuses on two major objectives. Under the finance section of the charter it focuses on the financial policies, strategies and capital structure. In the risk management section of the charter, it focuses on the company's risk management strategies and policies, including overseeing the management of market, credit, liquidity and funding risks, but its purpose clearly is not limited only to financial risks (See Figure 7) when viewed along with its responsibilities (See Figure 8).

GM's Audit Committee Charter contains a broad range of duties (27 specific duties) from auditing the financial reporting process and system to reporting GM's financial position and affairs. GM's policies and compliance procedures in GM's Audit Committee Charter is limited to two specific risks: ethics and legal risk identified in GM's compliance program. In addition, the Audit Committee is responsible for reviewing policies regarding risk assessment and risk management. Such review is to include GM's major financial and accounting risk exposures and actions taken to mitigate these risks, so there is a directed cross-responsibility with GM's Finance and Risk Committee.

## IS THE AUDIT COMMITTEE OR RISK COMMITTEE BETTER SUITED TO OVERSEE RISK?

ERM Strategies' comparative study revealed that not only was the Purpose section of both the audit and risk committee charters different, but the Duties and Responsibilities section also held significant differences. (See Figures 5 and 6)

Sample Board Committee Purpose	
<b>IIA Audit Oversight</b> <ul style="list-style-type: none"> <li>• Financial reporting process</li> <li>• System of internal control</li> <li>• Audit process</li> <li>• Monitoring process for compliance with laws and regulations</li> <li>• Code of conduct</li> </ul>	<b>NACD Risk Oversight</b> <ul style="list-style-type: none"> <li>• Risk management</li> </ul>

Figure 5

Sample Committee Responsibilities	
<b>IIA Audit Oversight</b> <ul style="list-style-type: none"> <li>• Review financial statements</li> <li>• Effectiveness of internal control system and scope of internal and external reviews</li> <li>• Internal audit function, audit plan, performance and effectiveness of IA staff</li> <li>• Review external audit plan and performance and effectiveness of external auditors</li> <li>• Review effectiveness of system for monitoring legal &amp; regulatory compliance, findings, process for communicating code of conduct</li> </ul>	<b>NACD Risk Oversight</b> <ul style="list-style-type: none"> <li>• Monitor all enterprise risks</li> <li>• Discuss major risk exposures and steps ... taken to monitor and control, including risk assessment and risk management policies</li> <li>• Review activities and consider risks that may affect the entire company's viability and steps taken to manage these risks within acceptable tolerances</li> </ul>

Figure 6

## GM Reality – Committee Purpose

GM Audit Committee Oversight	GM Finance and Risk Committee Oversight
<ul style="list-style-type: none"> <li>Integrity of financial statements</li> <li>Compliance with legal and regulatory requirements</li> <li>Qualifications and independence of external auditors</li> <li>Performance of GM's internal audit staff and external auditors</li> </ul>	<ul style="list-style-type: none"> <li>Financial policies, strategies, and capital structure, making such reports and recommendations to the Board as it deems advisable</li> <li>Risk management strategies and policies, including overseeing management of market, credit, liquidity and funding risks ("risks")</li> </ul>

Source: <http://www.gm.com/investors/>

Figure 7

## GM Reality – Committee Responsibilities

GM Audit Committee Oversight	GM Finance and Risk Committee Oversight
<ul style="list-style-type: none"> <li>Independent and objective monitoring of GM's financial reporting process and systems of disclosure and internal controls for effectiveness</li> <li>Review and appraise the audit process of GM's external auditors and internal audit staff</li> <li>Provide for open, ongoing communications regarding GM's financial position and affairs</li> <li>Review GM's policies and compliance procedures regarding ethics and legal risk</li> <li>Oversee preparation of Audit Committee Report for annual proxy statement</li> </ul>	<ul style="list-style-type: none"> <li>Financial matters, including insurance and risk management processes</li> <li>Risk appetite and risk tolerance, aggregate measurements and setting of limits and escalation actions</li> <li>Categories of risk, including concentrations and risk interrelationships</li> <li>Design of risk management functions</li> <li>Review implementation of risk policies and procedures for effectiveness</li> <li>Review internal communication systems</li> <li>Review internal and external reports regarding risks and risk management function</li> </ul>

Source: <http://www.gm.com/investors/>

Figure 8

GM's Finance and Risk Committee Charter states that the risk assessment and risk management are the responsibility of the company's management. The Committee's risk responsibility is one of oversight and review. In addition to the duties listed in the chart (Figure 8), the Committee is required to periodically receive reports regarding U.S. employee benefit plans, but the charter specifies that the Committee is not responsible for the oversight of the ERISA plans.

What's even more revealing with respect to how GM is tying its risk oversight with its strategy is found in the composition of GM's Finance and Risk Committee membership. (See Figure 9)

## GM Finance and Risk Committee Composition

<b>CHAIR</b> Daniel F. Akerson Chief Executive Officer General Motors Company Director since July 24, 2009	Erroll B. Davis, Jr. Chancellor University System of Georgia Director since July 10, 2009
<b>MEMBERS</b>  Stephen J. Girsky Vice Chairman, Corporate Strategy and Business Development General Motors Company Director since July 10, 2009	Philip A. Laskawy* Retired Chairman and Chief Executive Officer Ernst & Young LLP Director since July 10, 2009  Patricia F. Russo** Former Chief Executive Officer Alcatel-Lucent Director since July 24, 2009

Source: <http://www.gm.com/investors/>

Figure 9

The composition of the GM's Finance and Risk Committee is comprised of two "insiders": its CEO, its Vice President of Strategy and Business Development and three independent directors. The independent directors include the chairs of both the audit and executive compensation committee. By coordinating with the Chair of the Audit Committee, both the audit and the finance and risk policy committees are receiving all information necessary to permit them to fulfill their duties and responsibilities with respect to oversight of the risk assessment and risk management.

With the Chair of the Executive Compensation Committee also on the Finance and Risk Committee, this ensures that GM's compensation arrangements are designed to provide incentives that are consistent with the interests of GM's stockholders, but do not encourage senior executives to take excessive risks that threaten the value of the company.

In this way, GM has tied its risk oversight directly to strategy, audit and executive compensation. GM's Audit Committee Charter and Finance and Risk Committee Charter reflect GM's thought process in having the two charters complement and collaborate, but not compete. The charters:

- Complement each other on their risk oversight duties and responsibilities
- Collaborate through distinct and defined purpose, functions and roles, spelling out how the board committees will work together, and
- Are purposefully crafted so that the committees are not competing against each other on risk oversight purpose or responsibilities

## RESULTS OF RIMS WEBINAR POLL

So are risk committees becoming more prevalent for board oversight? In December 2010, RIMS conducted an instant poll (see Figure 10) with approximately 125 of the nearly 200 participants in its "Evolving Model for Board Risk Governance" webinar responding to the question "How does your organization's board discharge its risk oversight responsibilities?" as follows:

- 21% Full Board
- 32% Audit Committee
- 25% Risk Committee
- 7% Other Committee
- 15% No Formal Oversight

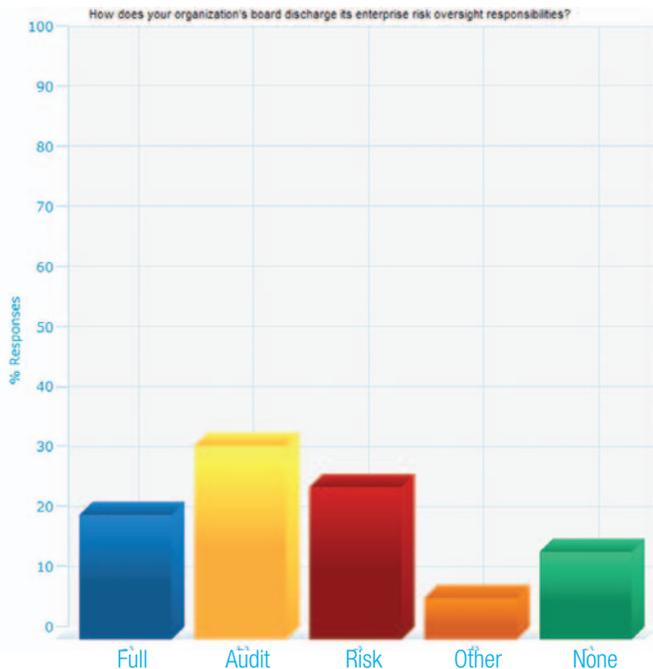


Figure 10

Since those responding that a separate risk committee is structured at the board level represented a higher than expected percentage, we reviewed publically available information to determine the types of organizations within the responding group that had verifiable board-level risk committees separate from the Audit Committee. The largest percentage of this smaller sample represented financial institutions, as expected. However, organizations in other sectors such as mining and biotech obviously have moved to board level risk committees, as well.

### A TRANSFORMATIVE MODEL FOR BOARD RISK GOVERNANCE

Based on this limited research, it appears that boards are transforming their governance models for deeper risk oversight. One size does not (and should not) fit all. In fact, a governance model including a risk committee may be just the place to focus risk issues in the context of strategic and operational objectives (See Figure 11).

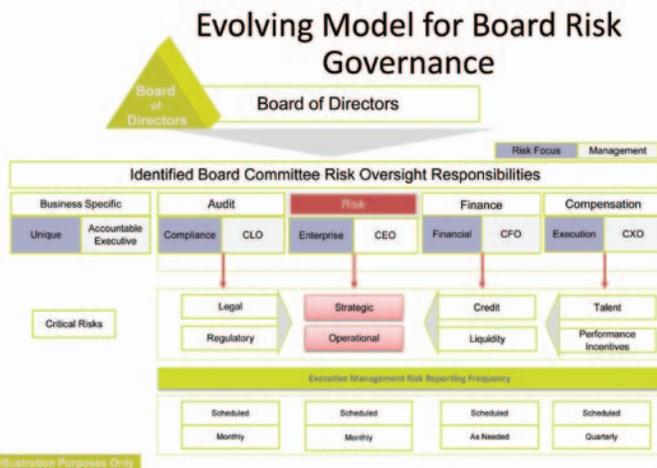


Figure 11

Most boards have, at a minimum, an audit, finance and compensation committee. These committees already focus on specific risks to the organization, such as legal, regulatory, financial and talent. These specific risks may be, but are not necessarily, critical to the achievement of the organization's strategic or operational objectives. On the other hand, there are risks that are uncovered through the ERM process that definitely rise to a strategic level. Some of the biggest risks identified in a recent Economist Intelligence Unit survey included weak demand, instability in major markets, financial market volatility and insolvencies among customer and supplier bases.<sup>11</sup> Oversight for assessment and management of these potential risk impacts on strategic objectives may not find a natural home among existing committee structures.

That is why some organizations have developed management level risk committees. It seems logical to have a complementary risk committee at the board level, as well, for oversight purposes. For some organizations, the entire board may want to be the de facto "risk committee." However, as noted with GM, the charter spelling out the purpose and responsibilities provides the necessary discipline to execute this oversight.

GM chose to combine its risk committee with its finance committee. Other organizations may choose to keep the board risk committee separate from the finance committee. If we follow the implied logic in the NACD recommendation, organizations may also include business specific committees that focus on critical risks to that organization. Some real examples include such "business specific" committees as GM's Public Policy Committee and Chiquita's Food Innovation, Safety & Technology Committee.

Structured and scheduled reporting from management prevents the risks related to strategy from being an afterthought. By directing these siloed risks into a focused structure that concentrates on the major risk impacts to strategic and operational objectives, the organization creates an enterprise risk management practice that:

1. Is viewed internally and externally as a business discipline that supports the achievement of an organization's objectives
2. Addresses the full spectrum of its risks and
3. Manages the combined impact of those risks as an interrelated risk portfolio.

Maintaining the balance between efficiency and effectiveness at the board level depends on the size and complexity of the organization and the board itself. However, one could argue that such a single purpose risk committee would actually improve the board's efficiency and effectiveness.

## CONCLUSION

By virtue of the combined governance drivers created over the last ten years, the evolving model of risk governance includes board member oversight responsibilities, *a structure in the form of a risk committee*, and a process in the form of enterprise risk management. Board risk committees:

- Serve a strategic function, while audit committees primarily serve a control function
- Need to collaborate with other board risk oversight functions, including audit and compensation committees
- Are becoming a best practice in good governance for driving value creation and protection, especially when tied to strategic objectives
- Require members with expertise in identifying, assessing and managing risks

Appropriate board structures to address risk oversight will continue to be fluid and dynamic as the regulatory agenda ebbs and flows with reactions to scandals and financial stress. Nevertheless, we anticipate that risk committees will become the norm in most public companies, as enterprise risk management becomes a standard discipline on a global basis.

## ABOUT THE AUTHORS:

Carol Fox is the director of strategic and enterprise risk practice for RIMS.

John Bugalla is principal of ermINSIGHTS, a consulting firm that specializes in enterprise risk management practices.

Kristina Narvaez is the president and CEO of consulting firm ERM Strategies.

## END NOTES

- <sup>1</sup> Risk Intelligent Proxy Disclosures: Transparency into Board-Level Risk Oversight, Copyright © 2010 Deloitte Development LLC.
- <sup>2</sup> 2010-2011 Policy Survey Summary of Results, Institutional Shareholder Services, Inc. Copyright © 2010 ISS; [http://www.issgovernance.com/files/ISS2010-2011\\_PolicySurveyResults.pdf](http://www.issgovernance.com/files/ISS2010-2011_PolicySurveyResults.pdf)
- <sup>3</sup> See Caremark, and Stone v. Ritter cases - Sullivan and Cromwell, Akin Gump, and Nixon Peabody
- <sup>4</sup> [http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/d/walker\\_review\\_261109.pdf](http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/d/walker_review_261109.pdf)
- <sup>5</sup> Canada: Corporate Governance Developments In Canada And The United States by Cornell Wright and Leslie McCallum, Torsys LLP, 10 February 10, 2011 © Mondaq® 1994-2011 [www.mondaq.com/canada/article.asp?articleid=122622](http://www.mondaq.com/canada/article.asp?articleid=122622) Ibid
- <sup>6</sup> Ibid.
- <sup>7</sup> United States Securities and Exchange Commission Proxy Disclosure Enhancements, effective date February 28, 2010 <http://www.sec.gov/rules/final/2009/33-9089.pdf> page 44
- <sup>8</sup> The Growing Role of the Board in Risk Oversight by Kevin M. Connelly, Carolyn C. Eadie and Valerie R. Harper, From Point of View ©2010 Spencer Stuart
- <sup>9</sup> National Association of Corporate Directors Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies, 2009
- <sup>10</sup> The interim committee was named the Finance and Risk Policy Committee.
- <sup>11</sup> Fall guys Risk management in the front line, © The Economist Intelligence Unit Limited 2010.



## About RIMS

RIMS is a not-for-profit organization dedicated to advancing the practice of risk management. Founded in 1950, RIMS represents some 4,000 industrial, service, nonprofit, charitable and government entities. The Society serves more than 10,000 risk management professionals around the world.



## About the ERM Center of Excellence

RIMS ERM Center of Excellence is the risk professional's source for news, tools and peer-to-peer networking on everything related to Enterprise Risk Management. Whether you are initiating an ERM program within your organization, in the implementation phase or streamlining processes, in RIMS ERM Center of Excellence you will gain access to the key information and connect with the risk practitioners that will put you on the road to ERM success.

The information contained in this paper is based on sources believed to be reliable, but we make no representations or warranties, expressed or implied, regarding its accuracy. This publication provides a general overview of subjects covered and is not intended to be taken as advice regarding any individual situation. Individuals should consult their advisors regarding specific risk management issues.

**RIMS**

1065 Avenue of the Americas  
13th Floor  
New York, NY 10018

Tel: 212-286-9292  
email: [ERM@RIMS.org](mailto:ERM@RIMS.org)  
[www.RIMS.org](http://www.RIMS.org)