THE CONFERENCE BOARD

RESEARCH REPORT

The Role of U.S. Corporate Boards In Enterprise Risk Management

R-1390-06-RR

The Conference Board creates and disseminates knowledge about management and the marketplace to help businesses strengthen their performance and better serve society.

Working as a global, independent membership organization in the public interest, we conduct research, convene conferences, make forecasts, assess trends, publish information and analysis, and bring executives together to learn from one another.

The Conference Board is a not-for-profit organization and holds 501 (c) (3) tax-exempt status in the United States.

To obtain additional copies of this report…

Members of The Conference Board can access an electronic version by visiting the Members Only Web site: www.conference-board.org/boarderm.htm

Additional printed copies of the full report can also be obtained by contacting customer service at 212 339 0345 or orders@conference-board.org

Non-members can purchase an electronic version or additional printed copies by visiting www.conference-board.org or calling customer service at 212 339 0345.

ACKNOWLEDGMENTS

The authors are indebted to the directors who shared their experience in the field and, particularly, to those who agreed to be personally interviewed (see list on page 31).

In addition, the authors would like to express their gratitude to the members of the Advisory Board to the project (see list on page 32), for their invaluable intellectual contribution to shaping the scope of the research and analyzing its findings.

Special thanks to André Brodeur, Kevin Buehler, and Gunnar Pritsch of McKinsey & Company, for their help in conducting the interviews. To them and to Kenneth Daly and Caryn Bocchino of KPMG's Audit Committee Institute and John M. Farrell and Scott A. Reed of KPMG LLP, many thanks for the insightful comments and suggestions at various stages of the process.

Also, thank you to Henry Silvert, Judit Torok, and Tam Hernandez for their assistance in preparing the survey and computing statistical data on responses.

ABOUT THIS **REPORT**

The Conference Board with McKinsey & Company and KPMG's Audit Committee Institute conducted research on the role of U.S. corporate boards in Enterprise Risk Management between October 2005 through February 2006. This research consisted of a combination of personal interviews with corporate directors, a written survey, an analysis of Fortune 100's board committee charters, and legal research on regulatory law and directors' fiduciary responsibilities. An Advisory Board was assembled to provide direction on the project.

THIS REPORT WAS PREPARED WITH THE INTELLECTUAL CONTRIBUTION OF MCKINSEY & COMPANY.

ABOUT **MCKINSEY & COMPANY**

McKinsey&Company

McKinsey&Company is a management consulting firm that helps many of the world's leading corporations and organizations address their strategic challenges, from reorganizing for long-term growth to improving business performance and maximizing revenue. With consultants deployed in more than 40 countries across the globe, McKinsey advises companies on strategic, operational, organizational and technological issues. For eight decades, its primary objective has been to serve as an organization's most trusted external advisor on critical issues facing senior management.

THIS REPORT WAS PREPARED WITH THE SPONSORSHIP OF KPMG'S AUDIT COMMITTEE INSTITUTE.

ABOUT **KPMG'S AUDIT COMMITTEE INSTITUTE**

KPMG's Audit Committee Institute (ACI) has been communicating with audit committees since its formation in 1999. Its programs have allowed ACI to meet directly with thousands of directors and officers. ACI's initiatives include semiannual roundtables, publications, conference and board presentations, a toll-free hotline, periodic distribution of time-sensitive information, and a Web site, www.kpmg.com/aci. ACI can be reached toll-free at 877-KPMG-ACI (877-576-4224) or via e-mail at auditcommittee@kpmg.com.

The Role of U.S. Corporate Boards in Enterprise Risk Management

by Carolyn Kay Brancato, Matteo Tonello, and Ellen Hexter, with Katharine Rose Newman

contents

ABOUT THE **AUTHORS**

Carolyn Kay Brancato, Ph.D., is Director of The Conference Board Governance Center and Directors' Institute and the author of two major books on corporate governance. She has been invited to speak on global trends in governance by leading corporate, investor and governmental organizations in more than 20 countries.

Before joining The Conference Board, Dr. Brancato was a securities analyst for a Wall Street brokerage firm, and later head of the Industry Analysis and Finance Section of the Congressional Research Service, United States Congress. In this position for nearly 10 years, she analyzed mergers and acquisitions, leveraged buyouts and major economic trends affecting U.S. industries for the United States Congress. She has also served as the Executive Director of the Columbia Law School Institutional Investor Project, the Staff Director for the U.S. Competitiveness Policy Council's Subcouncil on Corporate Governance and Financial Markets, and as Chief Economist for Weil Gotshal & Manges, a major international law firm. Dr. Brancato is a Fellow of the Royal Society for the encouragement of Arts, Manufactures & Commerce. She earned her B.A. degree in Economics from Barnard College, Columbia University and her Ph.D in Public Finance from New York University.

Matteo Tonello, LL.M, Ph. D., is Senior Research Associate of The Conference Board Governance Center. A qualified attorney in New York and Italy, he practiced corporate law at Davis Polk & Wardwell from 1998 to 2004.

Recently, Dr. Tonello advised the Italian National Commission on corporate governance reform on the effects of the Sarbanes-Oxley Act on foreign private issuers, and contributed to the drafting of the two final reports by the Commission. A new securities law enacted by the Italian Parliament in December 2005 was largely based on the Commission's findings and related recommendations. He is the author of two books in Italian, on international convergence of corporate governance standards and on the corporate veil piercing doctrine. For The Conference Board, he authored a report on stock market short-termism and a study of corporate governance best practices in family-controlled corporations.

Dr. Tonello received a Master of Laws degree from Harvard Law School and a J.D. from the University of Bologna. He also earned a Ph.D. in Law from the St. Anna Graduate School of the University of Pisa (Italy) and was a Visiting Scholar at Yale Law School in 1997.

Ellen Hexter, CFA, has been consulting for The Conference Board since 1991. She works with senior executives of major corporations, primarily finance and strategy executives, to set agendas and develop timely discussion topics for their periodic council meetings sponsored by the Board. Ms. Hexter manages seven of these executive councils at The Conference Board in addition to working in the research and conferences areas. She managed The Board's Working Group on Merger Effectiveness and was Project Director and co-author of The Conference Board's new report on ERM, "The Future of Risk Management: Beyond Compliance." Ms. Hexter also runs The Board's annual Enterprise Risk Management Conference and manages both the U.S. and European Strategic Risk Management Councils.

Ms. Hexter received an A.B from the University of Michigan and an M.B.A. from Cleveland State University. After receiving her M.B.A., Ms. Hexter began work as an equity securities analyst for Cowen & Co. in New York. Her career on Wall Street included positions as a corporate credit analyst and a mergers and acquisitions specialist. She is a Chartered Financial Analyst and serves as an arbitrator for the National Association of Securities Dealers.

Katharine Rose Newman was a research assistant on the project. She has almost a decade of experience with Cablevision Systems Corporation in the areas of customer relations and system functions analysis. Before relocating to Los Angeles, Ms. Newman was in facilities management, supervising daily building operations for the New York City offices and network studios of Rainbow Media Holdings, Inc. She received a B.A in English Literature and B.S. in Education, summa cum laude, from Long Island University at its C.W. Post campus.

Executive Summary

Boards of Directors in the United States, having focused heavily on Sarbanes-Oxley requirements and more rigorous governance and compliance standards, are now beginning to assess their evolving role in providing oversight in the area of enterprise risk management (ERM). In view of the rapidly developing state of ERM in U.S. corporations, boards face a particularly challenging set of issues in responding to the need for improved oversight of risk management. For these reasons, it seems timely and useful to assess how corporate boards will be moving from their current focus on internal controls to a more comprehensive ERM framework and, importantly, toward integration of this framework with their historic strategic oversight responsibilities.

The Conference Board's research (see Appendix I on page 30 for Research Methodology) documents these key trends:

- Evolving legal developments make it prudent for directors to ensure they have a robust ERM oversight process in place;
- An increasing number of directors acknowledge they must oversee business risk as part of their strategy setting role;
- Directors should consider making improvements in their ERM oversight processes;
- Sound ERM oversight and implementation practices are now recognizable in a number of leading companies; and
- Companies may be looking at best-in-class peers for emerging practices in ERM oversight.

Key Research Findings

1. Evolving legal developments make it prudent for directors to ensure they have a robust ERM oversight process in place and that they are proactive in their oversight of risk management processes.

Such developments involve:

- The interpretation of recent Delaware case law
- New York Stock Exchange Listing Standards
- SEC's endorsement of self-regulatory frameworks (i.e. COSO) to manage financial risk
- The new Exchange Act requirement to consider risk factor disclosure in annual and quarterly reports
- Federal Sentencing Guidelines reform
- Best practice standards being implemented in highly-regulated industries (e.g. banking and insurance)

In addition, rating agencies, institutional investors, and insurance companies underwriting directors' and officers' liability insurance policies are increasingly focusing on whether companies have ERM processes in place. This suggests that corporate boards may wish to re-assess their approach to risk oversight as a fundamental element of good governance.

2. An increasing number of directors acknowledge they must oversee business risk as part of their strategy-setting role.

- Just a few years ago, directors had a less-than-complete understanding of business risks, and research on implementation of Enterprise Risk Management showed companies were at early stages.
- Now, many more directors say they have a better understanding of the major risks faced by their companies.
- Nevertheless, most board members tend to resist excessive formalization of ERM oversight processes.
- Directors today believe strategic risk rather than financial risk is their key concern.
- An enterprise-wide, top-down approach to risk management is viewed as a strategic effort rather than merely a compliance practice.

3. Directors should consider making improvements in their ERM oversight processes.

Directors confirm that every conversation they have about strategy embodies issues of risk, and risk is discussed on a case-by-case basis in connection with specific strategies or events.

While most directors say they have a good or very good grasp on understanding risk implications of strategy, directors are less likely to appreciate how the different parts of a business interact in the company's overall risk portfolio.

Although those directors surveyed feel satisfied with their risk oversight and in the level of implementation by management, the personal interviews with directors show considerably less comfort in several key areas:

- Directors report a significant variation in knowledge of risk among their peers.
- Directors report a significant variation in practices among different industries.
- Less than half of the directors surveyed can point to the use of robust techniques to help them oversee risk and the majority of boards are not yet using a ranking system as part of their risk assessment practices.

4. Sound ERM oversight and implementation practices are now recognizable in a number of leading companies.

Responsibilities between the Board and Management

- The full board clearly has oversight responsibility for strategy as well as ERM. The agendas for both are set by management and approved by the full board.
- It is the board's responsibility to provide oversight and ensure that an effective process for identifying, assessing, and mitigating risks exists within the company.
- It is management's responsibility to see that risk management is embedded in everyday business decisions throughout the company on an enterprise-wide basis.
- At the senior level, in addition to the CEO, a risk management team may include the Chief Financial Officer or a Chief Risk Officer. Relatively few companies formally designate a Chief Risk Officer in their charters, although the practice is becoming more widespread.

Responsibilities among the full Board and Committees

- Two-thirds of companies currently delegate risk oversight responsibility to the audit committee. However, a small number of companies distinguish between financial risk and other business risk, and they additionally charge another committee with broader-based business risk oversight.
- Where one or more committees oversee risk, they should coordinate and report to the full board which maintains the overall strategic responsibility.

5. Companies may be looking at best-in-class peers for emerging practices in ERM oversight.

- Reported variations (from industry to industry and from company to company) in the sophistication of ERM oversight processes–especially among the financial and energy/utility industries–provide an opportunity to learn from those firms that are distinguishing themselves as leaders in ERM development.

Recommendations to Corporate Boards

Directors who are considering recommending that their companies upgrade their ERM capabilities may wish to consider the following recommendations:[1]

1. Review committee structure and charters.

To ensure effective risk management oversight, it must be clear where responsibility for it resides at the board level. Most companies currently lodge this oversight in the audit committee, however, some directors believe that this committee is overburdened and may not have the skills and focus to deal with enterprise-wide risks. In response, some companies have established a dedicated risk committee or have given risk oversight to an existing committee such as the governance committee. This committee then shares risk oversight with the audit committee, and both committees report to the full board where the ultimate responsibility for risk oversight resides. Many directors stated that risk oversight is so integrally linked to strategy oversight that it belongs primarily to the full board.

---

1 The survey and interview research did not specifically ask directors for their recommendations regarding ERM, however, based upon extensive work in governance and ERM, The Conference Board, together with McKinsey and KPMG's Audit Committee Institute, offer these recommendations.

2. Review the competencies of the Board in fulfilling its risk oversight duties.

   Strengthen the board, if needed, by ensuring it has the right people, a variety of expertise, and proper training. Management should proactively identify ways to "raise the risk management IQ of the board." Best practice examples include:

   - conducting risk management training for all board members (e.g., upon joining the board);
   - dedicating some time at each board meeting to discuss issues of particular relevance (e.g., the implications of the Basel II capital accord on banks); and
   - providing more analysis on the company's risk profile and the risk/return nature of decisions.

3. Develop a risk management process to ensure directors are fulfilling their fiduciary responsibilities and will, therefore, be afforded the protections of the Business Judgment Rule when making decisions.

   The process should ensure appropriate oversight with regard to management's enterprise-wide risk assessment, mitigating and monitoring. The process should begin with a review of the company's drivers of performance, and then continue with an inventory of risks and an analysis of how those risks will affect shareholder value.

4. A robust board level ERM reporting system should be considered.

   The design of board reports on risk begins with a clear understanding of what information the board and its committees need to understand and what they are expected to do with this information. What risks does the entire board need to understand? How often does it need to review them? What should be reviewed by the different committees (e.g., finance, audit, or risk committee)? And, for what purpose is management asking the board to consider these risks? Is management asking the board to help assess the risks, to satisfy a fiduciary responsibility, to give permission to address certain risk events, or to make some other decision? Moreover, the report should focus on providing real information—not just data. For example, the report should prioritize key risk issues and include management's assessment of those risks, including a transparent display of the trade-offs and decisions made by management, and their rationale. Finally, the board reports should be part of an "integrated reporting framework," i.e. business unit reports should aggregate to a company level risk report, and there should be consistency between management information flow and reporting and board reporting.

5. Develop a process to assess and monitor performance of the risk management process.

   Best practice boards periodically (e.g., once per year) review the effectiveness of the risk management processes at the board level. Some best practice boards have developed a self-assessment tool with which they rate the board risk management process against a number of criteria. The effectiveness of board committee structures and charters, how well board members believe they understand risk policies, and how productive the interaction with management is on risk are all examples of these criteria.

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

   Board members should identify the handful of executives who have the best perspective on the company's key risks and interact with them directly.

Report Findings

Beware a False Sense of Security and Spread Risk Oversight Among Board Committees

Evolving legal requirements make it prudent for directors to ensure their companies have a robust Enterprise Risk Management (ERM) oversight program. Research findings are based on a written survey and personal interviews of board members as well as an analysis of Fortune 100 board committee charters. While many directors believe they have a good handle on the risks their companies face, others tend to approach risk more on a case-by-case basis and, therefore, may not have adequately robust and systematic ERM processes.

Research also shows some industries such as banking and financial services tend to have more developed ERM processes and may therefore set the standard by which other industries will be measured.

ERM Oversight Processes Have Improved, but Directors May Be Functioning with a False Sense of Security

While ERM processes have definitely improved since McKinsey did a similar survey in 2002, there may be a false sense of security among those directors reporting that they have a full understanding of the company's risks. Data in 2002 showed that 36 percent of directors did not have a full understanding of the major risks facing their companies; by 2006, that decreased to 10.5 percent.

When personally asked, many directors said they approach risk on a case-by-case basis in connection with a specific strategic issue such as a merger or acquisition or the entrance into a new market. This may give rise to a false sense of security.

The research found significant differences in how directors understand risk and how their companies manage risk. Thus, while:

- 89.5 percent of directors say they "fully understand"* the major risks facing the company,
- only 73.4 percent say their companies manage risk "fully or very well."

Directors may have more of a top down understanding of risk. Research finds:

- Although 89.5 percent of directors say they fully understand the risk implications of the current strategy, just …
  - 77.4 percent of directors say they fully understand the risk/return tradeoffs underlying the current strategy;
  - 59.3 percent of directors understand how business segments interact in the company's overall risk portfolio;
  - 54.0 percent have clearly defined risk tolerance levels;
  - 47.6 percent of boards rank key risks; and
  - 42.3 percent have formal practices and policies in place to address reputational risk.

Directors are, however, sensitive to the need for additional information:

- While 71.8 percent of directors believe they have the right risk metrics and methodologies in making strategic decisions;
- 47.6 percent of directors would like to see more data analysis related to the company's risk profile.

* "Fully understand" is defined as directors marking either a 5 or a 4 on a scale of 1-5, with the highest ranking being a 5.

Certain Industries, such as Banks and Insurance Companies, Tend to Have More Robust ERM Processes

Directors interviewed note significant variations in ERM capabilities among companies on whose boards they sit:

- 72.6 percent of directors serving on multiple boards see significant variations across firms in terms of their ERM capabilities; and
- Directors in financial companies tend to report more robust ERM practices. For example, 63.6 percent of financial company directors report their companies have clearly defined risk tolerance levels versus 46.7 percent for non-financial company directors (compared with 53.8 percent for all directors).

Financial service company directors also report a higher level of routine consideration of all major risks compared to considering risks only when management brings them to the board.

- 54.5 percent of financial directors report the board considers all major risks including strategic risks versus only 25 percent of non-financial directors (compared with an average of 39.1 percent for all directors).
- 27.3 percent of financial directors report they consider risks primarily when management brings them to the board, versus 50 percent of non-financial directors (compared with an average of 39.1 percent for all directors).

This may be a function of the fact that risk issues are historically considered in connection with the products of these banks and insurance companies. Nevertheless, standards used in the banking and insurance industries may set the pace for all companies. This factor may be increasingly important to directors in determining their exposure to liability for failing to meet their fiduciary duties—as the courts may increasingly look to comparative "best practice" standards by which to measure directors' performance of fiduciary duties of care, loyalty and good faith.

The Audit Committee Should Not Be the Sole Repository for ERM Oversight

The board committee charter analysis of Fortune 100 companies indicated that 66 percent of corporate boards place risk responsibility in the audit committee. In considering the organizational aspects of ERM board oversight, it is clear that the audit committee is the most common place to lodge ERM oversight responsibility. However, audit committees are already overburdened with their basic financial reporting risk responsibilities and boards should consider giving the more operational aspects of ERM to another committee to coordinate with the audit committee. Then, these two committees should report to the full board. In fact, research showed that, in addition to the 66 percent of companies where the audit committee is the sole repository of risk oversight, in 23 percent of companies another committee shares this responsibility with the audit committee.

Of the directors surveyed, 16.1 percent in the financial services area report having a separate and distinct risk committee for more than 2 years, versus 3.5 percent in the non-financial area (compared with 6.3 percent for all directors).

The CFO Is the Executive Who Most Frequently Informs the Board, Although Companies Are Beginning to Establish the Position of Chief Risk Officer

In addition to the CEO, the executive in the company most frequently cited by directors as responsible for informing the board on risk issues is the CFO (70.9 percent of companies). A Chief Risk Officer is cited as the person informing the board at 11 percent of companies (16.1 percent at financial and 7.1 percent at non-financial companies). This finding reinforces the notion that most directors are still equating business risk with financial risk, therefore missing the holistic component of Enterprise Risk Management. As companies move toward an integrated risk management environment, awareness about the importance of a dedicated reporting line on business risk will increase.

What Is

Enterprise Risk Management?

The most widely recognized definition of Enterprise Risk Management (ERM) is contained in COSO's 2004 *Enterprise Risk Management – Integrated Framework*. ERM is described as a process:

- Effected by an entity's board, management and personnel
- Applied in strategy setting
- Applied across the enterprise
- Designed to identify potential events that may affect the entity
- Designed to manage risks to be within the company's risk appetite
- Able to provide reasonable assurance regarding achievement of entity objectives
- Geared to the achievement of objectives in one or more separate but overlapping categories– it is "a means to an end, not an end in itself."[2]

Key Steps in Implementing an ERM System

There is considerable debate concerning how to start an ERM process. Members of The Conference Board Research Working Group "Enterprise Risk Management and Corporate Governance: A Risk-Based Approach to Corporate Long-Term Valuation" recommended that ERM should not be seen as an entirely new and separate infrastructure separate from the costly implementation of the internal controls procedures required by the Sarbanes-Oxley Act.[3] Instead, they recommended tying risk analysis to the company's existing financial and non-financial performance drivers of success[4] (often done in some kind of "dashboard"[5]). Others argue, however, that basing risk analysis on pre-determined performance criteria could impair the company's ability to cast a wide enough net in identifying risk issues.

Assuming that the ERM system starts out with key success drivers, additional steps should include:

- Relating these drivers of performance to the company's stream of revenues and earnings, as well as to its state of liquidity and vulnerability to a liquidity crisis.
- Drawing up an inventory of risk factors pertaining to each driver of success (see box *Elements of a Risk Inventory*).
- Devising a "heat map" of earnings vulnerability across business units (see Exhibit 1 *Risk "Heat Map" and Implications*).
- Arraying earnings vulnerabilities and probabilities graphically to track potential effects of various risks (see Exhibit 2 *Comparison of PSEG Risks for 2004*).

2 Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, September 2004, available at http://www.coso.org/publications.htm. In August 2004, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission issued its *Enterprise Risk Management – Integrated Framework*, expanding on the popular *Internal Control – Integrated Framework* of 1992. As the foreword to the new publication explains: "While [the ERM framework] is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to [it] both to satisfy their internal control needs and to move toward a *fuller risk management process*." (Emphasis added)

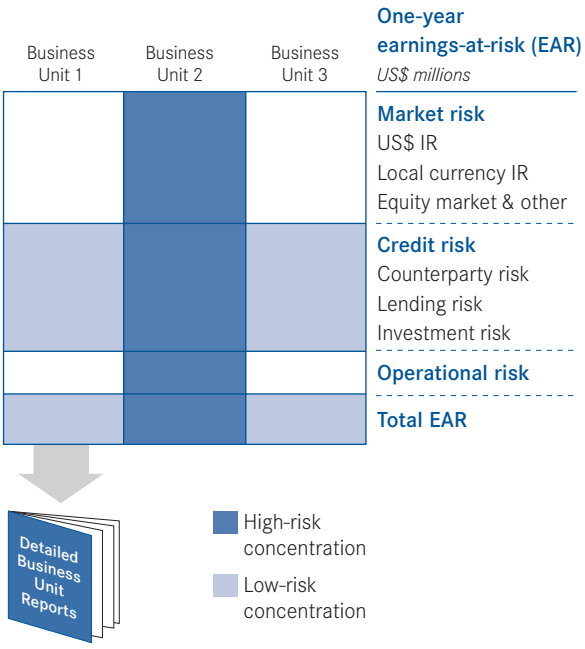
3 See Matteo Tonello, *Emerging Corporate Governance Practices in Enterprise Risk Management*, The Conference Board, Working Group Report, 2006 (forthcoming).

4 Carolyn Kay Brancato, *Enterprise Risk Management Systems: Beyond the Balanced Scorecard*, Special Report E-0009-05-RR, The Conference Board, 2005.

5 See Carolyn Kay Brancato, *Communicating Corporate Performance: A Delicate Balance*, Research Report 1188, The Conference Board, 1997; and *New Corporate Performance Measures*, Research Report 1118, The Conference Board, 1995.

Exhibit 1

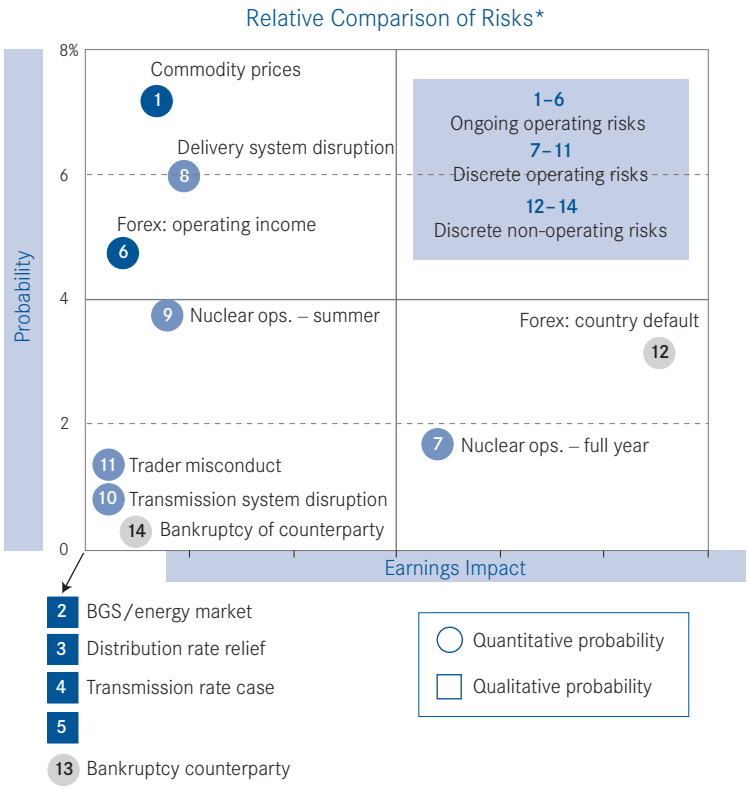
Risk "Heat Map" and Implications



Source: McKinsey & Company

Exhibit 2

Comparison of PSEG Risks for 2004



Observations

- The severity of either a country default or full-year nuclear outage is significantly higher than the other risks identified, with both being relatively lower probability events.
- The higher probability risks are associated with fluctuating commodity prices, fluctuating foreign exchange rates, and delivery systems disruptions associated with significant storms.
- Most of the on-going operating risks identified have little to no chance of impacting results during 2004, but emerge as significant risks over the five year plan timeframe.

* Quadrants reflect midpoints of axes for simple comparison.

Presentation by Laura L. Brooks, Vice President and Chief Risk Officer, PSEG, The Conference Board, September 22, 2004

Elements of a Risk Inventory

Financial Risks

- Market risk
- Credit Risk
- Liquidity Risk
- Fraud

Operational Risks

- Product risks
  - Raw materials
  - Design/engineering
  - Supply chain
  - Manufacturing operations
  - Compliance with legal and regulatory standards
- Distribution channels
- Information security
- Business continuity

Business Risks

- Technological disruption
- Disintermediation
- Changing terms of Competition

Governance and Human Resource Risks

- CEO succession
- Employee relations
- Compliance with laws, regulations and the company's governing documents on business conduct and ethics

Source: Debra Perry, Director, MBIA, Inc. and Conseco, Inc., Presentation, The Conference Board's Global Corporate Governance Research Center, Audit Committee Executives Workshop, September 22, 2004

Key Findings

Evolving legal developments make it prudent for directors to ensure they have a robust ERM oversight process in place.

Directors should be proactive in their oversight of risk management processes. A number of recent legal and regulatory developments are redefining directors' duties and strengthening executive accountability in the area of risk management (see Appendix II for a more complete discussion).

The Delaware Court of Chancery is evolving in its interpretation of the duties of care, loyalty, and good faith that define director responsibility. Recent decisions emphasizing the importance of compliance with best practices may be applicable to the enterprise risk management area.

The August 2005 *Disney* decision by the Delaware Court of Chancery provides some important insights into the scope of fiduciary duties (see box, "Directors Must Act in Good Faith"). While upholding the validity of the Business Judgment Rule, Chancellor William Chandler III underscored the importance of good faith in the performance of corporate duties and stated that directors and officers are expected to fully understand current best practices as well as ensure that business decisions are taken in light of widely-recognized corporate governance standards.[6]

The immediate implication of the *Disney* decision in the area of Enterprise Risk Management is that, even though they are just emerging, risk management best practices do matter and could be a standard of review of fiduciary liability.

Directors Must Act in Good Faith

The Business Judgment Rule protects directors who act in good faith from liability.

- It is designed to encourage business risk undertakings
- It focuses on the decision-making process
- Disinterested directors' decisions are not disturbed (other than in exceptional situations) if no breach of fiduciary duties has occurred

Directors' fiduciary duties include a duty to act in good faith.

- "Good faith" is an evolving concept
- Definitions contained in the 2005 Walt Disney case include:
  - "The good faith required of a corporate fiduciary includes not simply the duties of care and loyalty..."
  - "To act in good faith, a director must act at all times with honesty of purpose and in the best interests and welfare of the corporation."
- There are potential consequences for a breach of the duty:
  - director decisions may be set aside
  - personal liability for board members

Directors will be perceived as not acting in good faith if they take actions characterized as:

- Intentionally taken for a purpose other than company's best interests
- Intentional violation of applicable law
- Conscious and intentional disregard of a known duty
- Beyond the bounds of reasonable judgment
- "Sustained or systematic failure…to exercise oversight"
- "Knowing or deliberate indifference…to act faithfully and with appropriate care"
- Failure to exercise business judgment

Source: Alan A. Rudnick, Program Chair, The Conference Board Directors' Institute, presentation, March 8, 2006.

6 *In re Walt Disney Co. Derivative Litig*., Cons. C.A. No. 15452, 2005 Del. Ch. LEXIS 113 (Del Ch. Aug. 9, 2005). The judiciary interpretation of the Disney case should be read in connection with the principle, established in the earlier Caremark case, that a board has an obligation to "exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations" (*In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del Ch. Sept. 25, 1996)).

Key legal developments militating in favor of greater director oversight of ERM processes include the following:

Revised New York Stock Exchange Listing Standards requiring risk assessment and management policies

The revised Listing Standards require listed companies' audit committees to "discuss policies with respect to risk assessment and risk management" and, more specifically, to discuss their companies' "major financial risk exposures and the steps management has taken to monitor and control such exposures."[7]

SEC's endorsement of self-regulatory frameworks (i.e. COSO) to manage financial risk

SEC regulation enacted under Section 404 of the Sarbanes-Oxley Act (SOX) requires companies to design internal control and disclosure procedures according to a "suitable, recognized control framework"; specifically, the SEC recommends the use of the COSO 1992 *Internal Control – Integrated Framework.* By doing so, the SEC implicitly endorsed COSO's approach to managing financial fraud risks, where internal control is "a process, effected by an entity's board of directors, management and other personnel." While it states that SOX requirements are limited to the area of internal control and the risk of fraud, the SEC clearly encourages management to pay attention to a broader spectrum of risks, and to manage them in an enterprise-wide context.

The new Exchange Act requirement to consider risk factor disclosure in annual and quarterly reports

The SEC has extended to periodic filings on Form 10-K and Form 10-Q the same requirement to consider risk factor disclosure that had long been applicable—under Regulation S-K—to securities offering prospectuses.[8] The formulation of the requirement is vague and does not explicitly suggest that the company should disclose the knowledge of risk it acquired through its risk management processes. Nonetheless, discussion of such factors in annual and quarterly reports should highlight major risk issues for the attention of investors and financial analysts. Ultimately, the market demand for periodic updates on risk may increase the pressure on the company to establish a comprehensive ERM infrastructure.

Federal Sentencing Guideline amendments requiring the establishment of a corporate compliance program addressing, among other things, risk issues

Amendments to the Federal Sentencing Guidelines (effective as of November 1, 2004) provide for a more lenient treatment of corporate crimes if the organization had established a well-functioning and qualifying compliance program. Although no specific compliance program is described, it must be regularly revised and appropriately modified to address new areas of risks to which the corporation is exposed.[9]

Best practice standards implemented in highly-regulated industries (e.g. banking and insurance)

As certain industries—especially banks and insurance companies—adopt leading "best practices," this may encourage legal interpretation that best practices should be more universally adopted by companies in industries not prone to developing robust risk oversight processes.

Rating agencies are more attuned to companies' ERM systems

Finally, while not a facet of law or regulation, institutional investors have increasingly focused on risk management and rating agencies such as Moody's and Standard and Poor's have begun to incorporate risk management assessments into their credit rating decisions. Insurance companies underwriting directors' and officers' liability insurance also pay attention to rating agency opinions. These developments suggest that corporate boards may wish to re-assess their approach to risk oversight as a fundamental element of good governance.

---

7 Section 303A of the NYSE Listing Manual.

8 See Item 1A of Securities Exchange Act Forms 10-K and 10-Q, effective December 1, 2005. For the requirement to disclose risk factors already applicable to Securities Act registration statements and prospectuses, see Item 503(c) of Regulation S-K.

9 See Chapter Eight ("Sentencing of Organizations"), Amendment 673 (Supplement to Appendix C) *2004 Federal Sentencing Guidelines Manual*, available at http://www.ussc.gov/2004guid/tabconchapt8.htm. For an overview of the United States Sentencing Commission and the Federal Sentencing Guidelines, see http://www.ussc.gov/general/USSCoverview_2005.pdf

An increasing number of directors acknowledge they must oversee business risk as part of their strategy-setting role.

Just a few years ago, directors had a less-than-complete understanding of business risks, and research on implementation of Enterprise Risk Management showed companies were at early stages.

For example, a 2002 McKinsey/Directorship Magazine survey[10] (involving 200 directors representing over 500 boards, and released just before the Sarbanes-Oxley Act was enacted into law) found that board members were concerned about their companies' ability to manage risk (see Exhibit 3). Specifically:

- 43 percent of directors said their process to identify, safeguard, and plan for key risks was either non-existent or ineffective
- 36 percent said they only had a partial understanding of the major risks facing the company
- 73 percent said they supported an increase in the audit committee's responsibility for risk management
- 52 percent supported the creation of a separate risk management committee

The study also showed that non-financial risks received only "anecdotal treatment" in the boardroom.

The Conference Board management research conducted in 2004[11] involving 271 companies based in North America and Europe confirmed the existence of significant shortcomings in corporate ERM processes (see Chart 1):

Exhibit 3

Four years ago, a McKinsey survey of 200 corporate directors highlighted the need to strengthen risk management at the board level

"I don't really know what's going on."

— U.S. director of mid-cap company

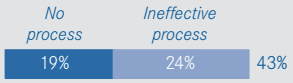
Many directors lack a full understanding of the major risks facing their business…

Does your board understand major risks facing the company?

Percent without a full understanding of risk

…and also lack the processes to oversee those risks.

Does your board have in place processes to identify, safeguard, and plan for key risks?

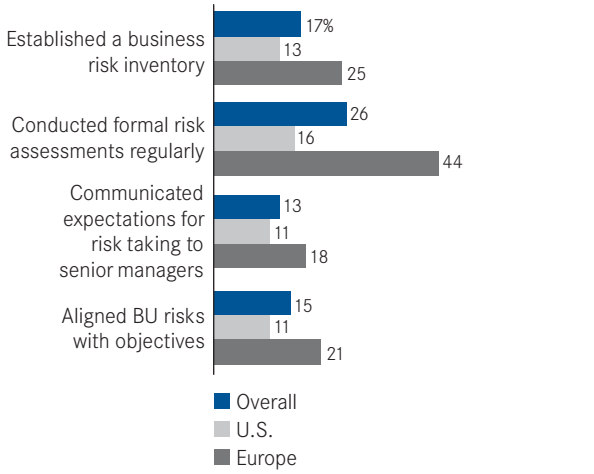


Source: McKinsey & Company

Chart 1

Progress on Developing Enterprise Risk Management Practices

2004 Conference Board survey of 271 companies in North America and Europe



Source: Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, The Conference Board, R-1363-05-RR, 2005

10 Robert Felton and Mark Watson, *U.S. Director Opinion Survey on Corporate Governance 2002, Presentation of Survey Findings*, McKinsey 2002. Findings are also discussed in Robert Felton and Mark Watson, *Informed Change*, Directorship, June 2002; and Robert F. Felton and David W. Anderson, *Directors and Investors Favor Further Governance Reform, not Regulation*, Directorship, October 2003. The study was based on 170 responses to a written questionnaire and 25 oral interviews.

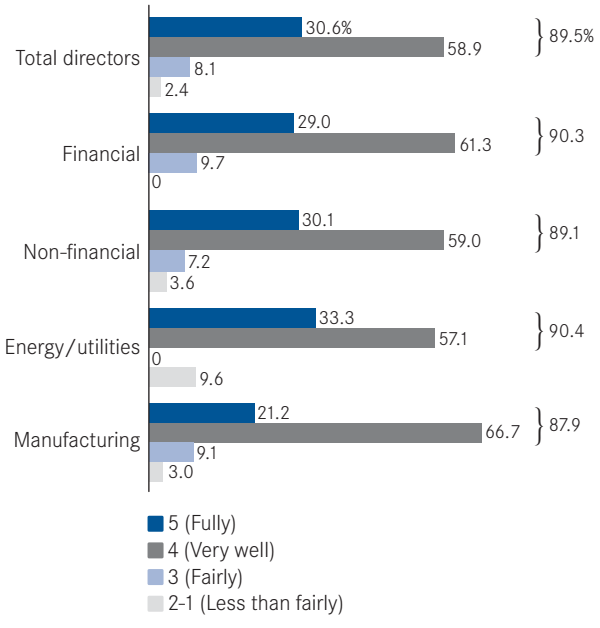
11 Stephen Gates and Ellen Hexter, *From Risk Management to Risk Strategy*, Research Report R-1363-05-RR, The Conference Board. The report was based on a 2004 survey of North American and European business leaders undertaken by The Conference Board and Mercer Oliver Wyman.

- In spite of a positive disposition toward ERM, most companies were still at early stages of implementing it. The survey indicated that only 18 percent of companies had the most basic element of Enterprise Risk Management in place: that is, the compilation of a business risk inventory. Moreover, 14 percent said they had developed a common language for risk exposure, making it the least common foundational component of ERM.
- Most companies were not yet achieving all expected benefits. While 86 percent of respondents with advanced practices believed that ERM has the potential to enable better informed decision-making, only 58 percent had already achieved this benefit.
- Only 16 percent of respondents have integrated advanced ERM thinking into business practices such as strategic planning or budgeting. Even fewer companies (4 percent) have driven ERM integration into performance metrics or compensation policies.
- Few companies (11 percent of the surveyed population) had fully developed ERM throughout all aspects of their operations; this minority reported a significantly increased level of perceived return from their efforts.

Chart 2

Directors' Understanding of the Company's Major Risks

On a scale of 1 to 5, with 5 highest



Percentages may not add to 100 percent due to rounding.

In contrast to just a few years ago, many more directors now say they have a better understanding of the major risks faced by their companies.

Of the directors surveyed as part of the 2005–2006 research project, 30.6 percent believe they "fully" understand the major risks faced by their companies, while another 58.9 percent say they have a "very good" understanding[12] (for a total of 89.5 percent of directors with a high degree of confidence—see Chart 2). Findings are relatively consistent among industries. However two trends stand out:

- Directors affiliated with companies in the manufacturing sector are more reluctant to state that they are fully comfortable with the risk inventory compiled by their organizations.
- Confirming previously-reported trends,[13] surveyed financial company board members appear to have a better understanding of business risk (none reported a "less than fair" degree of understanding) than directors in other industries.

Survey findings show a similarly high degree of familiarity by board members with:

- links between key risks and capital structure
- risks embedded in the company's operations
- relative importance of key risk factors
- new types of risk assumed by the company
- risk implications of new capital investments or acquisitions
- impact of risk on the company's overall cash flow volatility

12 On a 5 point scale 5 = "fully understands" and 4 = has a "very good understanding."

13 With regard to the comparative analysis, it should be noted that, in The Conference Board/Mercer Oliver Wyman 2004 survey, companies in the financial services sector (including banking and insurance businesses) represented 16.0 percent of the total surveyed population. Due primarily to the regulatory pressure to address financial risk exposure, financial companies are known to be more advanced in their internal control and enterprise risk management practices; leading standards in the banking sector, for instance, were reported by the Federal Reserve as early as 2001: see Christine M. Cumming and Beverly J. Hirtle, *The Challenges of Risk Management in Diversified Financial Companies*, Federal Reserve Bank of New York, Economic Policy Review, March 2001. Therefore, the larger percentage of financial firms participating in our 2005-2006 survey (26.7 percent of the total; see Research Methodology, at page 30) may help explain the reported confidence of many directors in their company's ability to effectively manage major risk issues.

Directors today believe strategic risk rather than financial risk is their key concern.

Of the directors surveyed, 53.3 percent believe "strategic risk" poses the greatest threat to the company, while only 15.7 percent indicate "financial risk" as their key concern (see Chart 3).

These findings show an increasing confidence on the adequacy of corporate financial controls. Reassured by the recent investment made to increase financial transparency and strengthen ethical standards, board members now seem more inclined to focus their monitoring role on other, more strategic, types of business risk.

This data may also be seen as the sign that corporate organizations have learned from the first few years of implementation of internal control procedures (mandated by Section 404 of the Sarbanes-Oxley Act) and are moving forward to a wider look at enterprise risk.

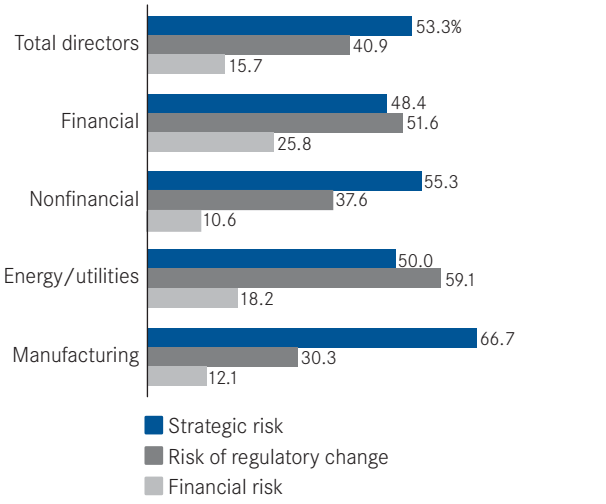
According to nearly 20 percent of surveyed directors, companies are "fully" managing their risk portfolios; another 54 percent say the portfolio is being managed "very well" (for a total of 73.4 percent with a high degree of comfort) (see Chart 4).

An enterprise-wide, top-down approach to risk management is viewed as a strategic effort rather than merely a compliance practice.

The research focused on the nature of the risk management oversight effort that many directors seem to consider increasingly important. Given the most recent emphasis on compliance practices developed to abide by Section 404 of the Sarbanes-Oxley Act, directors were surveyed to learn whether their perception of ERM truly reflects the strategic component assigned to it by the COSO Framework.

Chart 3

Directors say these are the risks that pose the greatest threat

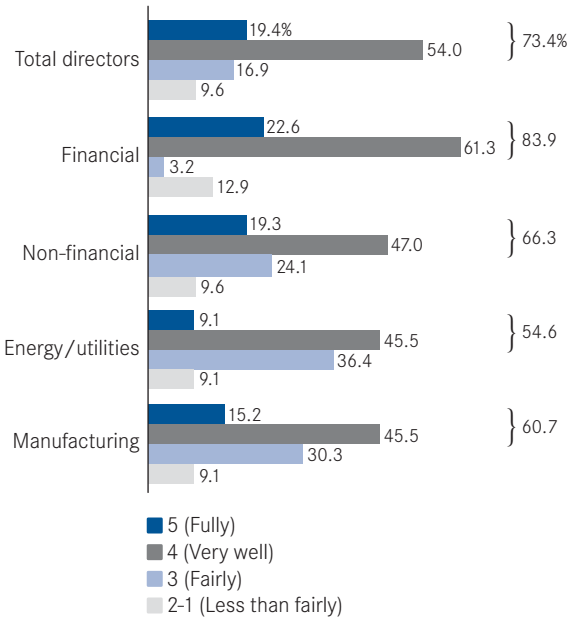


Multiple answers per participant; percentages will exceed 100 percent since participants may select more than one factor.

Chart 4

Degree to which directors believe their companies manage risks

On a scale of 1 to 5, with 5 highest



Percentages may not add to 100 percent due to rounding.

A number of questions in the survey asked about directors' awareness of the correlation between risk assessment and mitigation, strategic value creation and compensation policies. As Chart 5 indicates, directors have a strong grasp of such a correlation; moreover, they are in favor of using sound risk analysis techniques to refine or revise the company's long-term strategic objectives. (see Chart 5.)

These findings were then probed in personal interviews with directors. The companies with more systemized risk management infrastructures, such as MetLife, Inc., Wachovia Corporation, and MBIA, Inc., confirmed their view of enterprise-wide risk management as a strategic effort. One director, actively serving on four boards, explained that, as companies develop and "move forward with their handling of ERM," directors' perceptions of risk management oversight evolve from a compliance practice to an exercise that is meant to bring clarity, focus and efficiency to the strategy-setting role of the corporate board. Another director explained that compliance is perceived as a precursor to full-fledged ERM, suggesting that companies need to "crawl before they can walk" in developing their risk management.

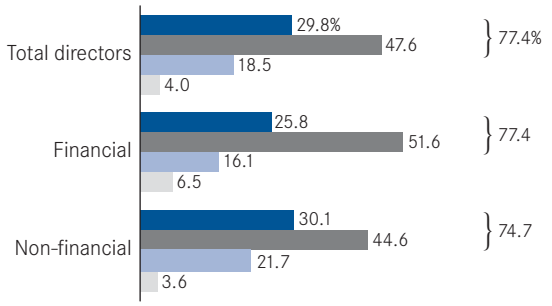
Nevertheless, most board members tend to resist excessive formalization of ERM oversight processes.

Many directors interviewed resisted what they termed "an excessively formal" way to incorporate risk management into their deliberations. Some reacted negatively to what they perceived to be another in a series of overly bureaucratic requirements such as Sarbanes-Oxley section 404 documentation requirements. Among the arguments for not wanting to formalize ERM processes, directors said: "ERM efforts are just being driven by the consultants," and "we can't separate risk as a separate topic from what we do."

Chart 5

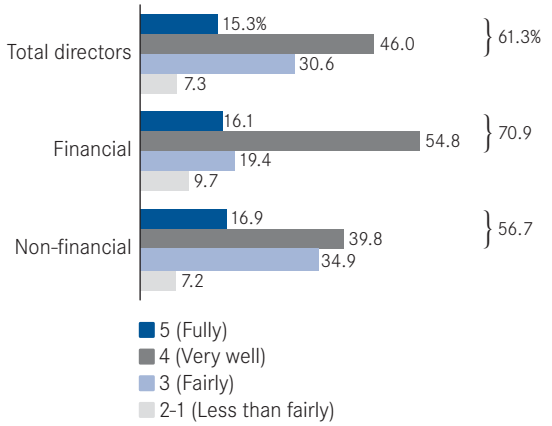
How well does the board understand how business risks could impede the implementation of the current corporate strategy?

On a scale of 1 to 5, with 5 highest

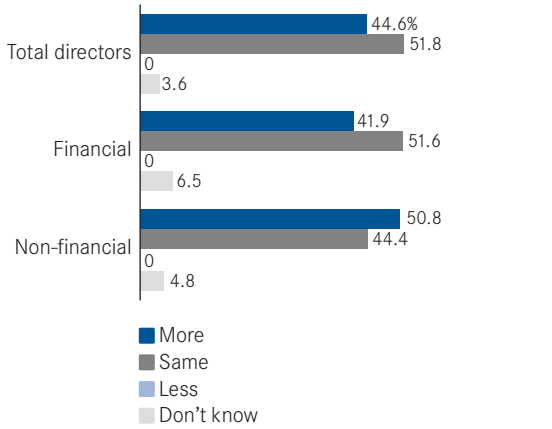


How well does the board understand potential conflicts between the corporate strategy, risk occurrence, and the executive compensation policy?

On a scale of 1 to 5, with 5 highest



Would the board like to see more or less risk analysis pertaining to the corporate strategy?



Percentages may not add to 100 percent due to rounding.

Directors should consider making improvements in their ERM oversight processes.

Directors confirm that every conversation they have about strategy embodies issues of risk, and risk is discussed on a case-by-case basis in connection with specific strategies or events.

Most directors say risk discussions take place in virtually every board meeting and executive session but they are not necessarily identified as "ERM or Risk Management" discussions on the agenda. Directors consistently say that they consider risks when discussing various strategic issues put before the board, such as an acquisition or an entry into a new market. However, they tend to consider these risks more on a case-by-case basis. Most did not wish to overload boards with general risk discussions, unrelated to specific events. Finally, most directors agree that risk management should not be a "separate" function—it should be embedded in everyday business decisions throughout the company.

Many directors also fear that focusing on risk as a separate process will segment out risk discussions when considering the business itself. One director noted: "Too much process takes away the focus on substance; risk issues surface when we discuss specific strategies or activities."

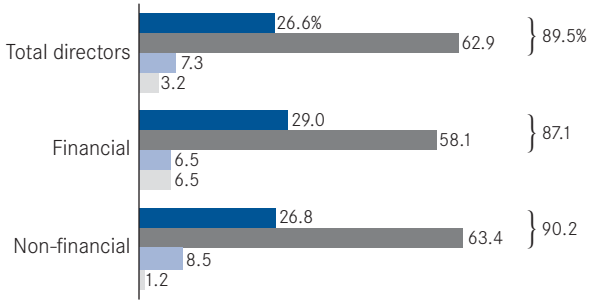
While most directors say they have a good or very good grasp on understanding risk implications of strategy, directors are less likely to appreciate how the different parts of a business interact in the overall company's risk portfolio.

Although directors are increasingly comfortable about the "major" and "top-line" risks their organizations face, they are less likely to appreciate how the different parts of a business interact in the overall company's risk portfolio. Chart 6 shows directors have a higher understanding of the risk implications of the current corporate strategy and the risk/return tradeoffs underlying this strategy compared with their understanding of how business segments impact the overall company's risk portfolio.

Chart 6

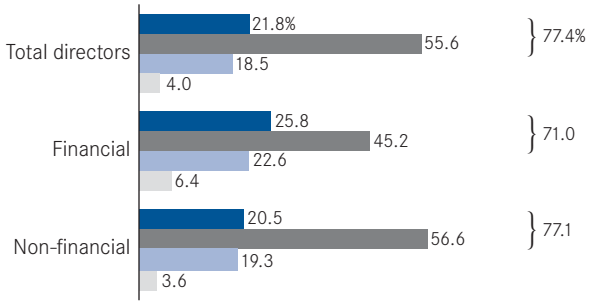
How well does the board understand the risk implications of the current corporate strategy?

On a scale of 1 to 5, with 5 highest



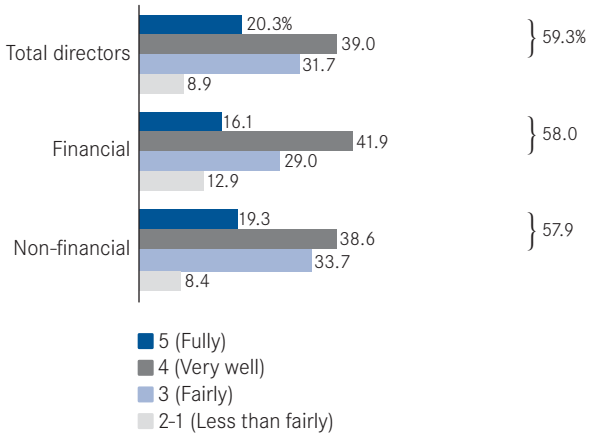
How well does the board understand the risk/return tradeoffs underlying the corporate strategy?

On a scale of 1 to 5, with 5 highest



How well does the board understand how business segments interact in the overall company's risk portfolio?

On a scale of 1 to 5, with 5 highest



Percentages may not add to 100 percent due to rounding.

Thus, only 20.3 percent report a "full" understanding of such interaction, and another 39.0 percent report a "very good" understanding, for a total of only 59.3 percent of directors with a high degree of comfort on the interplay of risks within several business segments.

Although those directors surveyed feel optimistic in terms of their comfort level with their risk oversight and in the level of implementation by management, the interviews with directors showed considerably less comfort in several key areas:

- Directors report they see significant variation in knowledge of risk among their peers;
- Directors report significant variation in practices between different industries; and
- Few directors can point to the use of robust techniques to help them oversee risk and the majority of boards are not yet using a ranking system as part of their risk assessment practices.

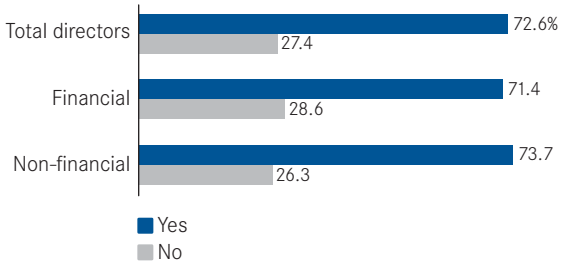
Directors sitting on multiple boards also report significant variations across firms in terms of their ERM capabilities.

In addition, among the individuals who sit on boards with more advanced ERM practices, many observed that some of their peers are "missing the point" on ERM (which ultimately is to improve a company's performance by providing decision-makers with insights on how risks are linked with value). On the other hand, it is commonly understood that the actual level of integration between risk and strategy depends on the nature of the industry, the company's history and culture, and the director's set of qualifications, skills and prior expertise.

Of directors surveyed, 72.6 percent say they see significant variations across firms in terms of their ERM capabilities (see Chart 7).

Chart 7

If you serve on multiple boards, do you see significant variations across firms in terms of their ERM capabilities?



Despite their overall comfort regarding their organizations' abilities to manage risk, directors report a wide variety of approaches to overseeing such management, ranging from highly formalized and quantitative to informal and qualitative.

The interviews reveal that boards of directors take many approaches to overseeing risk management processes established by their firms. Most consider reputational risk (see box below). Directors mentioned a variety of oversight practices, ranging from the establishment of *ad hoc* risk committees to unstructured risk discussions that rely primarily on situational tactics and gut feelings. In the second case, it became clear that, although directors thought they were responding to questions on ERM oversight, some companies are still using a fragmented, silo-based approach to risk management.

At a minimum, directors acknowledged the need to review management of those financial risk issues addressed by new internal control procedures. Where satisfied with this minimum, it is evident that the board has not fully understood the fundamental difference between a reformed, SOX 404-compliant, auditing process and the holistic, portfolio view of business risk that ERM implies.

Protecting the Firm's Reputation

Most companies address reputational risk. While half have formal processes, half do not.

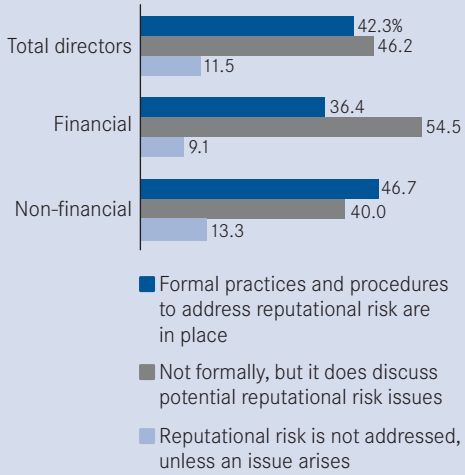
In examining how companies handle risk assessment and boards' roles in decision-making processes, directors were asked what actions their companies are taking to address reputational risk. Of the directors surveyed, 88.5 percent (90.9 percent for the financial category; 86.7 percent for the non-financial segment) say their boards address reputational risk. Half of the surveyed directors say they have formal practices. Half do not (see Chart 8).

When asked about whether or not the board specifically addresses reputation risk, one director replied that, "…this is a huge issue for us on the environmental side. We have had some employee litigation on safety in the past but are now the industry leader in safety."

Another Director, Ralph Larsen of General Electric Company and Xerox Corporation noted, "Reputation risk is embedded in every product or management decision. When considering some action, from new product introduction to a major downsizing, the board will certainly ask what the reputation risk is likely to be."

Chart 8

Is your company taking any action specifically to address reputational risk?



Less than half of directors surveyed can point to the use of robust techniques to help them oversee risk and the majority of boards are not yet using a ranking system as part of their risk assessment practices.

Risk assessment, which is a basic component of any ERM framework, benefits from the adoption of some form of ranking system. Under the COSO model, for example, prioritizing key risks according to the degree of attention that they require is necessary to evaluate the sufficiency of the internal resources that may be devoted to the mitigation of such risks. Ultimately, a ranking system can be an important element in the process of determining the firm's risk tolerance.

Nonetheless, more than half (52.4 percent) of surveyed directors report that their boards do not have a ranking methodology for business risk factors. An equal percentage state that they do not have access to concise analytical information on risk impact, such as heat maps or scorecards.

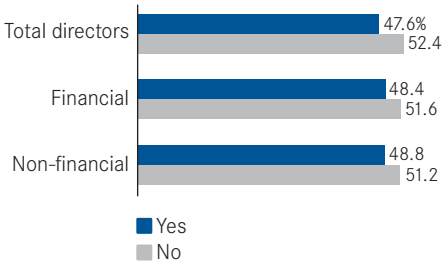
Finally, more than half of those that do rank key risks report that the review of such ranking occurs only annually.

It should be noted that findings on this specific point also applied to the financial industry (see Chart 9). These data may indicate that, although financial companies are often cited as the sources for emerging sound practices in ERM implementation, in at least half of them such implementation is still missing a fundamental component of a truly complete ERM process.

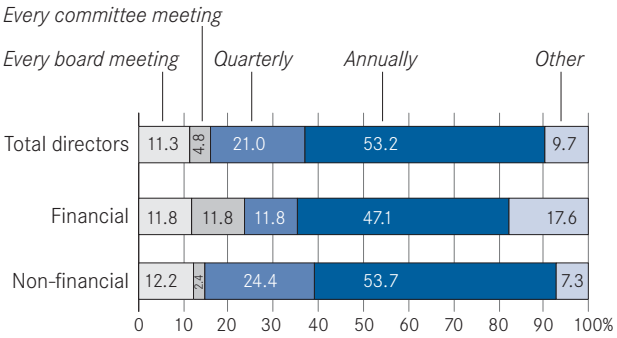
Interestingly, despite the lack of a risk ranking system, just over half of the directors interviewed confirmed their confidence about the risk tolerance level defined by the companies they are affiliated with (see Chart 10). These data contribute to the impression that there is a gap between the perception and the reality of ERM implementation in U.S. businesses.

Chart 9

Does the board rank key risks?



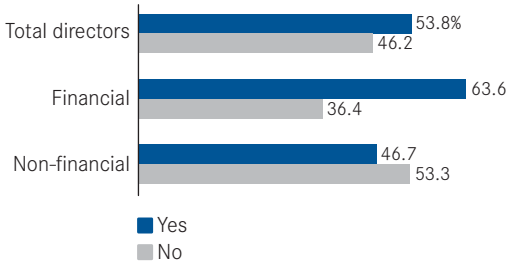
Except on an as-needed basis, how often does the board discuss this ranking?



Percentages may not add to 100 percent due to rounding.

Chart 10

Does your company have clearly defined risk tolerance levels?



Sound ERM oversight practices are now recognizable in a number of leading companies.

Responsibilities Between the Board and Management

The full board clearly has oversight responsibility for strategy as well as ERM. The agendas for both are set by management and approved by the full board.

Directors interviewed universally agree that the full board is responsible for strategy oversight. They confirm that it is the board's responsibility to provide oversight and ensure that an effective process for identifying, assessing, and mitigating risks exists within the company. It is management's responsibility to see to it that risk management is embedded in everyday business decisions throughout the company.

Directors repeatedly said that when it comes to risk management, tone at the top is critical. "Without tone at the top, a company can never have enough auditors, lawyers or compliance to make risk oversight work," says Jenne K. Britell, Chairman and CEO, Structured Ventures, Inc., and a director of Aames Investment Corporation; Crown Holdings Inc.; Quest Diagnostics, Inc.; and West Pharmaceutical Services, Inc.

Most of the directors believe that the responsibility for ensuring appropriate risk management lies with company management and the board is responsible to provide oversight to these processes. For example, three directors explained that boards instructed management to develop ERM approaches, identify risks, and address risk issues affecting the companies. The board then oversees management's agendas and processes. These directors agree that the board must be open to all presentations and discussions of risks that are deemed important enough for management to elevate them to the board level.

Of the directors surveyed, 80.5 percent say there is a clear agreement on the roles and responsibilities between the board and the management team regarding ERM. One former CEO, now serving on two large multi-national boards noted, "In my role as a director, my job is to protect the interests of the shareholders, not to protect management. We need to ask, 'Is what we are about to do in the long-term interest of shareholders?' Boards must ask management the 'what if?' questions."

Directors generally agree that the board should approve management's agenda, clearly defining what is expected, and allotting specific time for management to make presentations that display active involvement in identifying and assessing risks.

Most board members believe that risk management should be "second nature" for executives, i.e., their decisions should take into account how significant risks should be managed.

Directors are unanimous in the belief that the overall responsibility for ERM has to be with the CEO who must, in turn, infuse risk responsibility within the business units and line management. As one director put it, "you don't want your risks to be managed by a staff person—ultimately line management is accountable if something goes wrong." In a few exceptions, staff function may be accountable for risks, e.g., treasury department for currency risk. ERM accountability should be to ensure the risk management *process* is working. Hence, the role of a centralized ERM function is to provide support, tools, training to line managers who have to manage their risks.

But some directors may not be as proactive as they need to be. Of the directors surveyed, 39.1 percent (27.3 percent for financial; 50 percent for non-financial) still consider risks primarily when asked by management to review proposals, although another 39.1 percent (54.5 percent for financial; 25 percent for non-financial) of directors take a more proactive approach to reviewing risks (see Chart 11).

At the executive level, ultimate responsibility for risk lies with the CEO.

The risk management team is often led by the CFO and can include other officers such as the General Counsel, the Head of Internal Audit and the Chief Risk Officer (CRO). Relatively few companies formally designate a CRO in their charters, although there are signs that, over time, the practice is becoming more widespread.

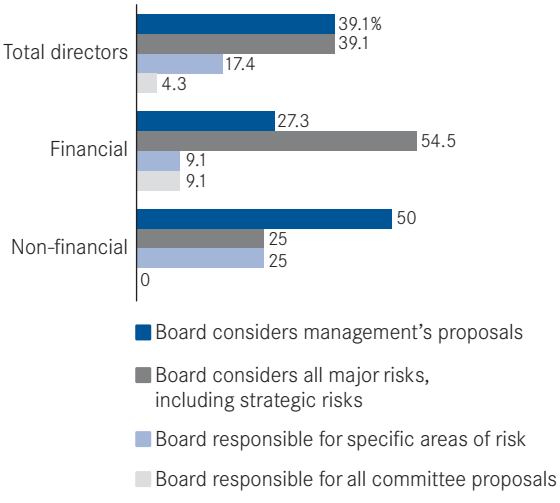
Of the directors surveyed, 69.7 percent are satisfied with their CEO's involvement in ERM and another 21 percent are somewhat satisfied. Only 5.9 percent and 2.5 percent are either "somewhat unsatisfied" or "very unsatisfied."

In addition to the CEO, findings indicate that the CFO is primarily responsible for informing the Board on risk issues, which reinforces the notion that most boards are still equating risk with financial risk. The directors surveyed indicate that in only 11 percent of the cases, the CRO is responsible for informing the board on risk issues (see Chart 12).

Respondents indicate a high level of satisfaction with the involvement in ERM of the CFO, the CRO, the General Counsel, the General Auditor and the external auditor. In addition, 32.5 percent of directors are very satisfied (and 40.4 percent are somewhat satisfied) with the involvement of business unit or segment leaders in ERM; while 14 percent don't know enough about their levels of involvement to express an opinion.

Chart 11

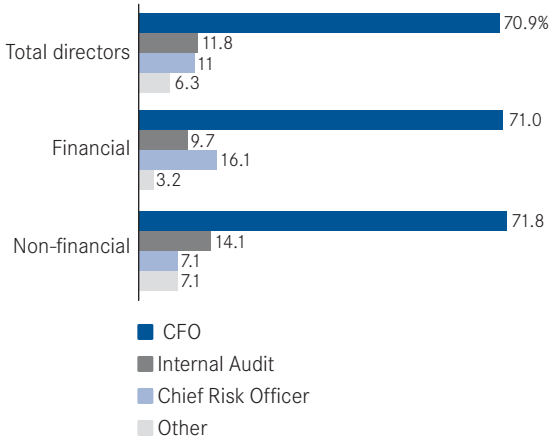
For what purpose is the board asked to consider major risks (e.g., satisfy fiduciary responsibilities, give permission to management, make a specific decision)?



Percentages may not add to 100 percent due to rounding.

Chart 12

In addition to the CEO, who in the company is primarily responsible for informing the board on risk issues?



Percentages may not add to 100 percent due to rounding.

Of the directors surveyed, most believe they have the right information to oversee risk management. More specifically, 71.8 percent fully or nearly fully (rank 5 and 4) believe that their companies use the right metrics and risk methodologies in making strategic decisions. Here again, confidence is greater for financial companies (83.9 percent) than for non-financial companies (65.1 percent) (see Chart 13). However, Chart 14 shows that nearly half of all directors would like more information.

Moreover, only 25 percent of surveyed directors receive either dashboards, risk rankings, or heat map information. Another 17.9 percent report receiving pre-meeting materials, publications, presentations addressing key risk issues, and additional supplemental information from audit reports and overviews of risks given to the audit and finance committees.

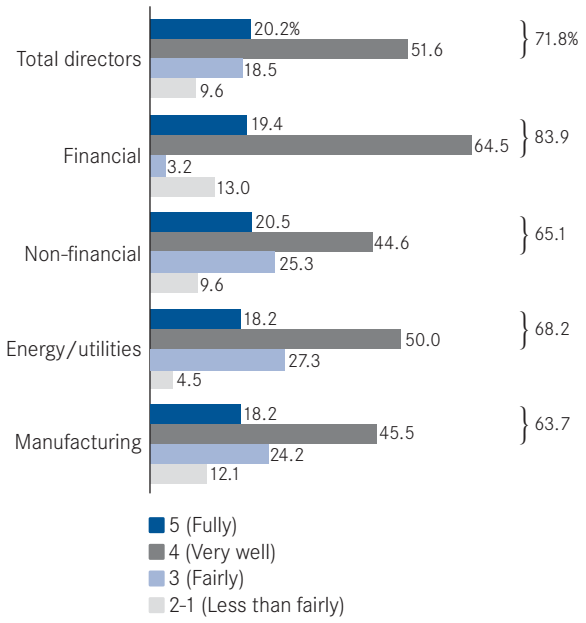
In order to manage their risks, there are some clear gaps in the information directors want to receive. Approximately 70 percent of respondents say management submits a concise, effective enterprise risk report that enables the board and its committees to fully understand critical issues. However, while 48.4 percent of the respondents are satisfied with the amount of data and analyses related to the company's risk profile that they receive from management, another 47.6 percent would find it helpful to receive more information.

In addition, as many as 55.3 percent of respondents believe that the amount of quantitative information they are provided on certain types of risks (financial, commodity, volume, operational) is adequate and should not be increased. As many as 40 percent, however, indicate that they would benefit from additional quantitative information (see Chart 14).

Chart 13

Does the company use the right risk metrics and methodologies in making strategic decisions?

On a scale of 1 to 5, with 5 highest

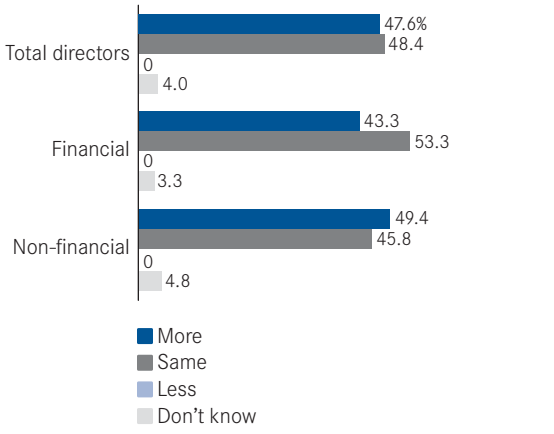


Percentages may not add to 100 percent due to rounding.

Chart 14

Would the board like to see more or less data and analysis related to the company's risk profile?

On a scale of 1 to 5, with 5 highest



Percentages may not add to 100 percent due to rounding.

Responsibilities Among the Full Board and Committees

Two-thirds of companies currently delegate oversight responsibility to the audit committee, however, a small number of companies additionally charge another committee with broader-based risk oversight.

Where one or more committees oversee risk, they should coordinate and report to the full board which maintains the overall responsibility for strategy and risk oversight.

In examining the committee charters of the Top 100 Fortune companies, 66 percent of company charters explicitly ascribe risk solely to their audit committees.[14] Another 23 percent of companies assign risk to the audit committee and to another committee which does not have risk in its title, while an additional 5 percent of companies assign risk to the audit committee and to another committee which does have risk in its title (see Chart 15).

Chart 15

Where do boards assign risk oversight?

Summary of top 100 company charter descriptions assigning risk

Companies where risks are assigned exclusively to Audit Committee	66%
Companies where risks are assigned to Audit and other committee[s] not identified as risk committee[s]	23
Companies where risks are assigned to Audit and other committee[s] identified as risk committee[s]	5
Companies that do not assign risk to any committee	3
Companies where risks are assigned to "partnered" Audit Committee without risk in committee title*	2
Companies where risks are assigned to "partnered" Audit Committee with risk in committee title*	1

* A "partnered" committee is a joint designation between the Audit and another committee. These categories refer to joint committees where risk is/is not included in the joint title.

The audit committees, already overburdened, may not have the skills to oversee an enterprise-wide risk management program which would be based on a wider range of issues than financial reporting and controls.

A group of companies assigns risk to an additional, separate risk committee so that the audit committee (which is charged with risk policy oversight) confers with the risk committee (which oversees operational enterprise-wide risk issues) in joint responsibility.

The industries where risk is most often shared among audit and other risk-designated committees are banking and insurance. The research shows that while 66 percent of companies have risk designated exclusively to the audit committee, none of the companies in the banking industry exclusively delegate risk to the audit committee—for all the banks, risk is shared by the audit committee and other committees (see Appendix III on page 38 for Individual Company Charter Analysis).

In comparison, non-financial companies have a higher tendency to lodge risk in their audit committees. Compared with an overall average of 66 percent for companies giving exclusive control over risk to the audit committee, 75 percent of companies in food, beverage and tobacco, 70.6 percent of companies in service industries, and 69 percent of manufacturing companies give risk to the audit committee. Companies which have established separate risk committees are shown in the box below.

Six Fortune 100 Companies Have Established Risk Committees

Wachovia Corporation (Risk Committee)

Citigroup, Inc (Audit & Risk Management Committee)

Duke Energy Corporation (Finance & Risk Management Committee)

St. Paul's Travelers Companies, Inc. (Risk Committee)

J.P. Morgan Chase & Company (Risk Policy Committee)

MCI, Inc. (Risk Management Committee)

In addition, **MetLife** has explicitly developed a risk framework which is overseen within the Governance Committee.

Source: Company committee charters from company websites. See Appendix III for summary of Charter analysis for Fortune 100 companies.

14 Separate survey findings confirm this trend, indicating 62 percent of director respondents say that that risk responsibilities are mostly assigned to the audit committee.

Specific elements of two bank's risk committee charters are shown in the following box.

Two Companies' Charters Contain In-Depth Descriptions of Risk Oversight

Wachovia Corporation

In addition to risk exposure and financial risk, charters included corporate risk exposures, strategy risk, reputational risk, liquidity risk, interest rate sensitivity risk, credit risk, operational risk, market risk, Chief Risk Officer, Credit Risk Committee, Market Risk Committee, Operational Risk Committee, Senior Risk Committee, fiduciary risk, finance risk, corporate risk management, market risks management.

J. P. Morgan Chase & Co.

In addition to risk assessment, risk management, charters included credit risk, market risk, fiduciary risk, corporate risk exposures, reputational risk, financial risk exposure, credit risk, market risk, interest rate risk, liquidity risk, investment risk, reputational risk, financial risk exposure, oversight of risk.

Source: Company committee charters from company websites: http://www.wachovia.com; http://www.jpmorganchase.com

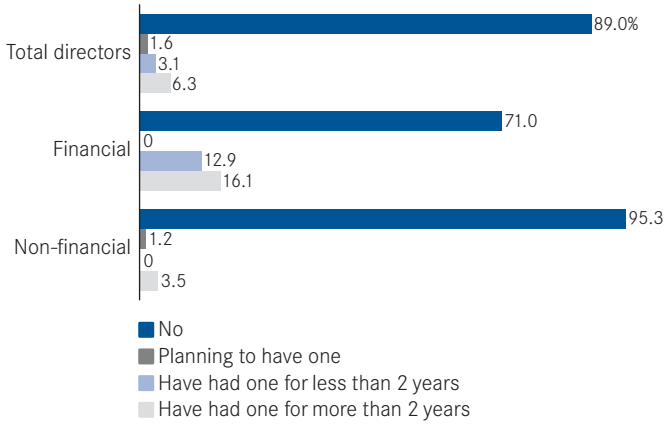
Directors are divided on whether there should be a separate committee to oversee risk.

When asked whether the board should centralize risk oversight in *one* committee responsible for risk oversight, 50 percent of directors (41.7 percent for financial and 56.3 percent non-financial) say there should not be a single separate risk committee. Of directors interviewed, 21.4 percent think there should be another committee besides the audit committee to handle risk and coordinate with the audit committee which should handle financial reporting risks—80 percent of these are in financial service/banking industries

The fear is that, by separating risk from other board efforts, it will not be as fully integrated as it is in current more qualitative strategy and operational discussions. These sentiments were reinforced by the survey which found 89 percent of directors say they do not have a separate and distinct risk committee. By comparison, in the financial industries, only 71 percent say they do not have a separate and distinct risk committee—a function of the regulatory structural aspects of these industries (see Chart 16).

Chart 16

Does your board have a separate and distinct risk committee?



Interview data roughly support the survey data in that 21.4 percent (33.3 percent for financial; 12.5 percent for non-financial) of directors say risk should be considered in a separate committee; 80 percent of these directors serve on financial service company boards. These directors noted that such a committee was already established, as at Wachovia. Furthermore, they argued that company-wide risks are too complex for the audit committee to manage exclusively—establishing a separate committee focus apart from the audit committee would most likely result in a more robust system of identifying and assessing risk management issues.

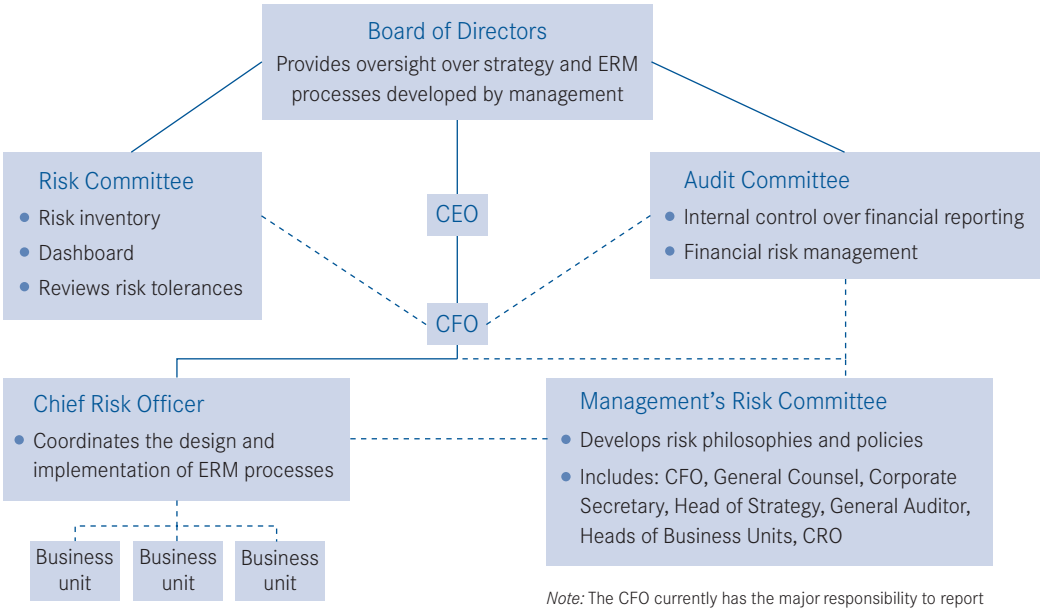
However, the audit committee should coordinate with any committee empowered to look at enterprise-wide risks and must still maintain risk oversight over financial reports and accounting policies.

Coordination is key among committees which handle risk and the full board which maintains overall oversight responsibility (see Exhibit 4).

This is the practice at MetLife—one of the few companies in the survey to have an established committee which specifically looks at risk—the Corporate Governance Committee. One director explained the rational for placing risk responsibility in multiple committees. At MetLife, the Corporate Governance Committee considers issues in broad areas such as operational risks while the Audit Committee focuses on finance-related risks, including risks associated with compliance and federal and state regulations. The company also has a management level Risk Policy Committee to handle risk pertaining to the company's investments and business transactions related to its corporate profit activities. The director noted that it is common for financial services companies, particularly banks and insurance companies, to have distinct management and, in some cases, board-level risk committees that focus on risk issues associated with the company's "products." Finally, 28.6 percent (25 percent for financial and 31.3 percent for non-financial) of directors are undecided on the best risk oversight structure.

Exhibit 4

ERM Responsibilities



Note: The CFO currently has the major responsibility to report to the board, but the CRO position is gaining in popularity.

Companies are looking at best-in-class peers for emerging practices in ERM oversight.

There are significant variations in level of sophistication among industries and companies, which provides an opportunity for some companies to learn from their best-in-class peers.

Industry and regulatory environment has an impact on a company's approach to risk management.

A few select industries are well ahead of their peers in developing and implementing their ERM processes. These industries, most notably banking, insurance, energy, and defense, tend to have more sophisticated risk management processes, primarily driven by heavy regulation.

That banks and insurance companies are at a more advanced stage of ERM development is understandable, given the regulatory constraints and the complexity of products in financial institutions. For example, Basel II guidelines (see Appendix II on page 33) require banks to establish a governance structure with independent validators checking risk models and auditors checking the independent validators. This might be regarded as overkill for a manufacturing firm.

Less sophisticated companies can learn from the more sophisticated ones. Early adopters in industries at the beginning of the learning curve can develop a competitive advantage by borrowing ERM practices from more sophisticated companies/sectors. A prime example is the energy sector, which has several characteristics in common with financial services—significant regulatory oversight and commodities that can be traded or hedged in the financial markets.

Appendix I

Research Methodology

The research was conducted between November 2005 and February 2006 and consisted of a survey, personal interviews, and an analysis of Fortune 100 companies' board committee charters. In addition, legal analysis was undertaken on the regulatory and legal framework defining directors' fiduciary duties. An Advisory Board of distinguished individuals was assembled to provide input to the project.

Survey-Based Research

A 32-question survey was disseminated to all U.S. corporate directors: (1) whose email and postal addresses are listed in The Corporate Library's Board Analyst database (a population of over 3,200 individuals); (2) attending The Conference Board Directors' Institute forum, held in New York City in November 2005; and (3) receiving KPMG biweekly newsletter, *Audit Committee Insights*.

A total of 127 directors responded to the survey, representing a response rate of approximately 4 percent. It should be noted that the survey included a number of complex and specific questions which may indicate that respondents were self-selecting for those who were most familiar with the subject. In the survey, directors sitting on multiple boards were explicitly asked to respond based on the company that, in their opinion, is the most advanced in the field. This may have contributed to an overly optimistic survey response when compared with responses provided by directors who were personally interviewed.

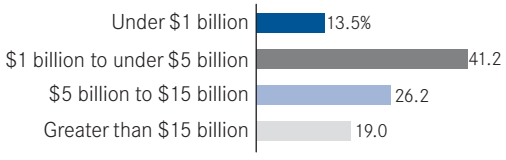
Where not stated otherwise, in this report we compressed survey findings for the energy/utility and the manufacturing sectors into a broader non-financial business category. This decision was taken, on a case-by-case basis, to facilitate the final analysis where results for the mentioned sectors appeared consistent with those for the remainder of the non-financial industries.

Interview-Based Research

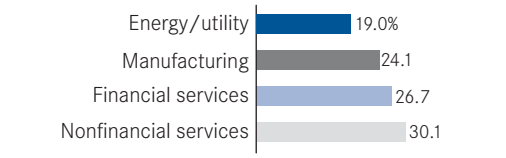
Thirty interviews were conducted, by phone or in person, with directors from a variety of industries, including financial services, retailing, food and beverage, technology, oil and energy, transportation, equipment manufacturing and general manufacturing. In the interviews, directors were asked to respond based on their overall board experience, not necessarily with regard to specific companies.

Sample by Size

(2004 Revenue)



Sample by Industry



Director Respondent Profile

N = 127

48.8%	On Audit Committee
25.2	Chairman of the Board
22.8	On Nomination (or Governance) Committee
15.0	Holds board responsibility in finance area
13.4	On Compensation Committee
8.7	Holds board responsibility in risk
4.7	Holds board responsibility in strategy/planning area

Interviewed Directors

Name	*Directorship*
Curtis H. Barnette	MetLife, Inc.
Frank J. Borelli	Interpublic Group of Companies, Inc. Marsh & McLennan Companies, Inc.* Genworth Financial, Inc.*
Jenne K. Britell	Aames Investment Corporation Crown Holdings, Inc. Quest Diagnostics, Inc. West Pharmaceutical Services, Inc.
Peter Browning	Nucor Corporation Lowe's Companies, Inc. Wachovia Corporation The Phoenix Companies, Inc. Acuity Brands, Inc. EnPro Industries, Inc.
Robert L. Burrus, Jr.	Smithfield Foods, Inc. S&K Famous Brands, Inc.
J. Michael Cook	Comcast Corporation Dow Chemical Company Eli Lilly and Company International Flavors & Fragrances Inc.
Curtis Crawford	El du Pont de Nemours and Company ITT Industries, Inc. Agilysys, Inc. ON Semiconductor Corp.
Alfred C. DeCrane, Jr.	Corn Products International, Inc.* Harris Corporation* CIGNA Corporation* Texaco Inc.**
Robert E. Denham	Chevron Corporation Lucent Technologies Inc. Wesco Financial Corporation Fomento Economico Mexicano S.A. de C.V. (FEMSA) United States Trust Company
Charles M. Elson	AutoZone Inc. HealthSouth Corporation Alderwoods Group Incorporated
John Fazio	ImClone Systems Incorporated Heidrick & Struggles International, Inc. Dendrite International, Inc.
Rita V. Foley	PetSmart, Inc. Council of the Americas Pro Mujer
Martha Clark Goss	Claire's Stores, Inc.
John R. Hall	GrafTech International Ltd. United States Enrichment Corporation (USEC, Inc.) Bank One Corporation* CSX Corporation* Canada Life* Humana Inc.* Reynolds Metals* Ashland Inc.**
John Johnstone	Arch Chemicals, Inc.* Research Corporation Technologies Inc.* Fortune Brands, Inc.* McDermott International, Inc.* Olin Corporation * Phoenix Companies, Inc.* Phoenix Life Insurance Company * Canadian Occidental Petroleum* Polysar Inc.*
Helene Kaplan	MetLife, Inc.
Olivia Kirtley	Alderwoods Group Inc. Papa John's International, Inc. ResCare, Inc.
Richard H. Koppes, Esq.	Apria Healthcare Group Inc. Valeant Pharmaceuticals International
Ellen J. Kullman	General Motors Corporation
Ralph Larsen	General Electric Company Xerox Corporation Johnson & Johnson**
Philip R. Lochner, Jr.	Apria Healthcare Group Inc. CLARCOR Inc. CMS Energy
Irene R. Miller	Inditex S.A. Coach, Inc. Barnes & Noble, Inc. The Body Shop International Plc. Oakley, Inc.* Benckiser N.V.*
Debra Perry	Conseco, Inc. MBIA, Inc.
Marla S. Persky	Cytyc Corporation
Kenneth Potashner	Newport Corporation V-Audit Corporation cVideo Corporation
Lowell W. Robinson	Jones Apparel Group, Inc. International Wire Group Diversified Investment Advisors, Inc.***
C.R. (Dick) Shoemate	Chevron Corporation International Paper Company*
Lizanne Thomas	Krispy Kreme Doughnuts, Inc.
Dennis P. Van Mieghem	Old Republic International Corporation

One director interviewed asked The Conference Board not to disclose his identity.

* Former Director

** Retired Chairman and CEO

*** Member of the Board of Trustees

Committee Charter Analysis

Board committee charters were examined to determine the extent to which committees are formally responsible for discussing business risk issues. The comparative analysis was limited to those Fortune 100 corporations whose committee charters were available on the companies' corporate websites.

Advisory Board for the Project

A distinguished Advisory Board was formed which provided input into shaping the scope of the project and commented on drafts of the report. The Advisory Board was composed of:

Curtis H. Barnette, Of Counsel, Skadden, Arps, Slate, Meagher & Flom; Director: Metlife, Inc.

Mark Beasley, Professor of Accounting and Director, Enterprise Risk Management Initiative, North Carolina State University

Peter Browning, Non-Executive Chairman: Nucor Corporation; Director: Lowe's Companies, Inc, Wachovia Corporation, Phoenix Companies, Inc. Acuity Brands, Inc. EnPro Industries, Inc.

Helene Kaplan, Of Counsel: Skadden, Arps, Slate, Meagher & Flom; Director: MetLife, Inc.

Debra Perry, Director: Conseco, Inc. and MBIA, Inc.

Appendix II

The Legal Foundation of Enterprise Risk Management[15]

The financial disruptions of the last few years revealed the inability of many business organizations to effectively assess and manage the risks they are exposed to. Stemming from those corporate *debacles*, a number of recent legal, regulatory and best practice developments are redefining director duties and strengthening executive accountability in the area of risk management.

The Expanding Scope of Fiduciary Duties under Delaware Law

Under state law, directors owe fiduciary responsibilities to the corporation and its shareholders. Traditionally, the corporate law of Delaware (which is where a vast majority of Fortune 500 businesses are incorporated) has required directors to act with loyalty to the corporation and exercise care in the performance of their duties.

The Business Judgment Rule is often cited as the main standard of review of director conducts by Delaware courts. By establishing a presumption that directors did act loyally and diligently, the business judgment rule is the crucial legal foundation of risk undertaking. Because of the protection they receive from the rule, directors are encouraged to embrace entrepreneurial risks and pursue the strategic opportunities originated by those risks.

The August 2005 *Disney* decision by the Delaware Court of Chancery provides some important insights into the scope of fiduciary duties. While upholding the validity of the Business Judgment Rule, Chancellor Chandler underscored the importance of good faith in the performance of corporate duties and stated that directors and officers are expected to fully understand current best practices as well as ensure that business decisions are taken in light of widely-recognized corporate governance standards.[16]

The immediate implication of the *Disney* decision in the area of enterprise risk is that, even though they are just emerging, risk management best practices do matter and could be a standard of review of fiduciary liability. To be sure, the judiciary interpretation of the *Disney* case should be read in connection with the principle, established in the earlier *Caremark* case, that a board has an obligation to "exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations."[17]

In the post-*Disney* state law environment, directors should consider the benefits of overseeing the development of risk management best practices and remain apprised of the state of the art in the area. Accordingly, executives and senior managers will likely be responsible for the implementation of risk management processes as well as for ensuring that there is an adequate flow of information to the board and shareholders on risk factors and events affecting business operations.

15 Source: Matteo Tonello, E*merging Corporate Governance Practices in Enterprise Risk Management*, The Conference Board, Working Group Report, 2006 (forthcoming).

16 *In re Walt Disney Co. Derivative Litig.*, Cons. C.A. No. 15452, 2005 Del. Ch. LEXIS 113 (Del Ch. Aug. 9, 2005). For a statutory requirement to act in good faith, see Section 102(b)(7) of the Delaware General Corporation Law, which permits a corporation to include in its articles of incorporation a provision eliminating or limiting a director's personal liability for monetary damages for breach of fiduciary duty so long as there are no "acts or omissions not in good faith." The standard for determining whether one has acted in good faith may depend on the director's degree of personal knowledge and expertise; for further information, see Carolyn K. Brancato and Alan Rudnick, *The Evolving Relationship Between Compensation Committees and Consultants*, citing the recent *In re Emerging Communications, Inc Shareholder Litigation* decision by the Delaware Court of Chancery (2004 Del. Ch. LEXIS 70), where a director was found personally liable for breach of good faith because – due to its financial expertise – he was in a "unique position to know" that a merger price was not fair.

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

Federal and Regulatory Requirements

While it did not specifically mandate on risk management, the Sarbanes-Oxley Act of 2002 (SOX) was the Congressional response to the poor quality of corporate disclosure emerged from scandals and a wave of financial restatements. Among other things, the new statute requires chief executives to establish (and report on the effectiveness of) internal control and disclosure procedures.[18] As per the subsequent regulation enacted by the SEC, such a set of procedures should be designed according to a "suitable, recognized control framework"; specifically, the SEC recommends the use of the 1992 Internal Control–Integrated Framework released by the Committee of Sponsoring Organizations of the Treadway Commission (also known as COSO).[19]

Implicitly, the SEC endorsed the COSO approach to managing financial fraud risks, where internal control is "a process, effected by an entity's board of directors, management and other personnel"[20] and based on the mapping and assessment of the risks a company is exposed to. While it states that SOX requirements are limited to the area of internal control and the risk of fraud, the SEC clearly encourages management to pay attention to a broader spectrum of risks, and to manage them in an enterprise-wide context. See box below for more evidence supporting this interpretation.

An Implicit Endorsement of Enterprise Risk Manaagement

What follows is an excerpt from the SEC Release on Management's Report on Internal Control, issued on June 5, 2003. Even though the release reaffirms the principle that any regulatory action is bound to the scope of the Sarbanes-Oxley Act, the following passage is compelling as it reveals the Commission's view of internal control as a procedural component of enterprise risk management:

"A few of the commenters urged us to adopt a considerably broader definition of internal control that would focus *not only on internal control over financial reporting, but also on internal control objectives associated with enterprise risk management and corporate governance*. While we agree that these are important objectives, the definition that we are adopting retains a focus on financial reporting.... We are not adopting a more expansive definition of internal control for a variety of reasons. Most important, we believe that [the Sarbanes-Oxley Act] focuses on the element of internal control that relates to financial reporting. In addition, many commenters indicated that even the more limited definition related to financial reporting that we proposed will impose substantial reporting and cost burdens on companies. Finally, independent accountants traditionally have not been responsible for reviewing and testing, or attesting to an assessment by management of, internal controls that are outside the boundary of financial reporting."[21]

21 SEC Release Nos. 33-8238; 34-47986, June 5, 2003, at text accompanying note n. 49. Emphasis added.

18 See Section 404 of the Sarbanes-Oxley Act for statutory requirements on the management's report on internal control. Also see Section 302 for the annual certification about the establishment of internal control and disclosure procedures that SOX imposes on listed companies' CEO and CFO. For a commentary on the Sarbanes-Oxley Act and SEC Rules, see John T. Bostelman, *The Sarbanes-Oxley Deskbook*, Practicing Law Institute, 2006.

19 SEC Release Nos. 33-8238; 34-47986 ("Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports"), June 5, 2003, available online at http://www.sec.gov/rules/final/33-8238.htm, at text accompanying note n. 67.

20 See COSO, *Internal Control–Integrated Framework*, 1992, available at www.coso.org. In 1995, the AICPA incorporated the definition of internal control set forth in the COSO Report in Statement on Auditing Standards No. 78 (codified as AU §319 in the Codification of Statements on Auditing Standards).

In addition, to "enhance the content of Exchange Act reports and their value in informing investors and the market,"[22] the SEC has extended to periodic filings on Form 10-K and Form 10-Q the same requirement to consider risk factor disclosure that had long been applicable—under Regulation S-K—to securities offering prospectuses.[23] The formulation of the requirement is vague and does not explicitly suggest that the company should disclose the knowledge of risk it acquired through its risk management processes. Nonetheless, discussion of such factors in annual and quarterly reports should highlight major risk issues for the attention of investors and financial analysts; ultimately, the market demand for periodic updates on risk may increase the pressure on the company to establish a comprehensive ERM infrastructure.

Listing Standards

The New York Stock Exchange (NYSE) Listed Company Manual assigns to the company's audit committee the duty and responsibility to "discuss policies with respect to risk assessment and risk management."[24]

The committee's role is further clarified in the commentary accompanying the set of regulatory requirements. In the commentary, the NYSE staff acknowledges that it is the job of the CEO and other senior executives to manage risk, and that the audit committee should limit its involvement to a general discussion of guidelines and policies governing the whole process. Most important, the written interpretation reveals how the nature of the risk covered by the rule is more specific than enterprise risk. In fact, the concept of "risk assessment and risk management" is explained as "the steps management has taken to monitor and control… the listed company's major *financial risk* exposure."[25]

In addition, the need to address risk factors through a set of pre-designed procedures emerges from the section of the NYSE Listed Company Manual imposing the adoption and disclosure of a code of business conduct and ethics, which "can focus the board and management on areas of ethical risk, provide guidance to personnel to help them recognize and deal with ethical issues, [and] *provide mechanisms* to report unethical conduct…"[26]

Risk management functions are not contemplated by the NASD Rules.

Federal Sentencing Guidelines

In response to a mandate included by Congress in the Sarbanes-Oxley Act, the United States Sentencing Commission has strengthened the section of its guidelines on crimes by business organizations. Ultimately, the purpose of the guidelines is to reduce any disparity in sentencing and ensure, to the greatest possible degree, certainty of criminal punishment. To do so, the Commission devised a point-based system whereas a numerical value is attributed to an unlawful conduct according to its degree of severity and the criminal history of the individual. The nationwide implementation of the system started in January 1989.[27]

Effective November 1, 2004, the new Federal Organizational Sentencing Guidelines provide for offsetting points and a more lenient treatment of executive mal feasance if the organization had established a well- functioning and qualifying compliance program. Although no particular compliance program is described, it must be reasonably designed to promote "*an organizational culture* that encourages ethical conduct and a commitment to compliance with the law."[28] Specifically, under the guidelines

22 SEC Release No. 33-8591; 34-52056 ("Securities Offering Reform"), July 19, 2005.

23 See Item 1A of Securities Exchange Act Forms 10-K and 10-Q, effective December 1, 2005. For the requirement to disclose risk factors already applicable to Securities Act registration statements and prospectuses, see Item 503(c) of Regulation S-K.

24 Section 303A.07(c)(iii)(D) of the NYSE Listed Company Manual, available at www.nyse.com.

25 See Commentary to Section 303A.07(c)(iii)(D) of the NYSE Listed Company Manual, also available at www.nyse.com. Also see John T. Bostelman, "Legal Update on Risk Management Issues," Presentation to The Conference Board Working Group on Enterprise Risk Management, New York City, September 15, 2005. Emphasis added.

26 See Commentary to Section 303A.10 ("Code of Business Conduct and Ethics") of the NYSE Listed Company Manual. Emphasis added.

27 For an overview of the United States Sentencing Commission and the Federal Sentencing Guidelines, see http://www.ussc.gov/general/USSCoverview_2005.pdf.

28 See Chapter Eight ("Sentencing of Organizations"), *2004 Federal Sentencing Guidelines Manual*, available at http://www.ussc.gov/2004guid/tabconchapt8.htm. Emphasis added.

directors and officers would benefit from the criminal fine reductions if the corporation demonstrates that:

- It has identified areas of potential risks for criminal violations
- It has trained senior officials and employees in the pertinent legal standards and obligations
- It has provided "sufficient authority and resources" to compliance officers to discharge their duties, including monitoring the compliance program and reporting periodically to the board of directors on its effectiveness
- Its directors and officers have, in fact, assumed responsibility for the oversight and management of the compliance program
- The program contemplates a set of procedures protecting whistleblowers from retaliatory actions
- The program is regularly devised and appropriately modified to address new areas of risks the corporation becomes exposed to.

It should be noted that, in a recent decision, the Supreme Court ruled that the mandatory nature of the guidelines is unconstitutional. In particular, the requirement that judges should calculate fines by taking into account information (such as the severity of the crime) that may not have been among the facts persuading the jury to convict a defendant was deemed in violation of the Sixth Amendment right to trial by jury. Nonetheless, the guidelines remain valid as advisory principles, and most commentators agree that the Supreme Court ruling should have no immediate effect on the sentencing mitigation compliance program that the guidelines encourage.[29]

Risk-Based Capital Adequacy Frameworks in Regulated Industries (Banking and Insurance)

Bank and insurance companies have a central role in the financial markets and decide on the allocation of large resources. Their business failures may have tremendous implications on the global economy. Since they are a source of systemic risk, banking and insurance activities are subject to heavy regulatory regimes. Such regimes are primarily intended to prevent unnecessary risk exposure and to ensure that, when a risk materializes, it is adequately managed so as to avoid ripple effects on the worldwide financial system.

The New Capital Adequacy Framework for bank capital regulation, also known as Basel II[30] was designed to improve operational risk management practices adopted by financial institutions, especially in the area of credit risk. In fact, the main premise for the work of the Basel Committee on Banking Supervision is that banks are subject to a number of operating risks resulting from ineffective or failed internal processes.

Basel II provides a platform for much needed convergence of credit risk management practices in financial institutions.[31] Risk management is also the key differentiation from the approach used in the preexisting 1988 Basel Capital Accord, as bank capital adequacy is now assessed through a wider range of risk-sensitive standards.

Basel II was formally endorsed in June 2004 by Central Bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries, including the United States. On the other hand, because of its nature of international agreement, its implementation and enforcement depend on its adoption by way of formal legislation. The European Union has done so through the so-called Capital Requirement Directive,[32] which calls

29 See, for example, John T. Bostelman, "Legal Update on Risk Management Issues." For an overview, also see Carolyn K. Brancato, *Enterprise Risk Management Systems. Beyond the Balanced Scorecard*, The Conference Board, Research Report E-0009-05-RR, 2005 and Harvey L. Pitt, "Fine Print: SEC Penalty Plan Explains Price of Fraud," *Compliance Week*, 31 January 2006.

30 Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, June 2004. For further information and updates, visit the official website at http://www.bis.org/publ/bcbsca.htm.

31 For a few examples of pragmatic applications of the Basel 2 operational risk management framework, see Benedikt Wahler, "Process-Managing Operational Risk. Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II Framework," Johns Hopkins University Working Paper, January 2005, available at http://ssrn.com/abstract=674221.

32 European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council recasting Council Directive 93/6/EEC of 15 March 1993 on the capital adequacy of investment firms and credit institutions (COM(2004)0486 – C6-0144/2004 – 2004/0159(COD)), available at http://www.europarl.eu.int.

for full implementation by the beginning of 2008. In the United States, regulation on Basel II is being developed by the SEC and the Department of Treasury agencies (FED, FDIC, OCC and OTS). According to the announced timetable, Basel II would become the capital adequacy standard in 2009, but only for institutions with more than $250 billion in assets or more than $35 billion in foreign receivables.[33]

The insurance industry is far behind in the development of international risk-driven solvency standards. However, the European Union has tried to replicate the success of the Basel Committee initiative and promoted the Solvency Framework Project. Solvency I became effective among EU Member States as of January 2004 and provided an initial, more fragmentary, risk-based set of capital requirements for insurance providers operating in Europe.[34] The intention of Solvency II, which remains under development, is to focus on an enterprise risk management approach to operational uncertainties in the sector.[35] If successful, the Solvency II holistic approach to risk management could foster new federal reforms in the United States, where the insurance industry is regulated by the Insurer Model Act of 1992.

33 In addition, to prevent a sudden drop in capital levels, they will not be allowed to decline more than five percent per year in each of 2009, 2010, and 2011. On the issues raised by the New Basel Accord in the United States, see Marc R. Saidenberg and Til Shuermann, "The New Basel Accord and Questions for Research," Federal Reserve Bank of New York, Wharton Financial Institutions Center Working Paper No. 03-14, May 2003, available at http://ssrn.com/abstract=410322.

34 Directive 2002/13/EC of the European Parliament and of the Council of 5 March 2002 amending Council Directive 73/239/EEC as regards the solvency margin requirements for non-life insurance undertakings, Official Journal L 077, 20.03.2002, page 17-22.

35 For an overview, see Martin Eling, Hato Schmeiser and Joan T. Schmit, "The Solvency II Process: Overview and Critical Analysis," Universitat St Gallen Working Paper, December 2005, available at http://ssrn.com/abstract=869267.

Appendix III

How Companies Designate Risk Among Committees–Organized by Industry[36]

Company[37] Committee Charter Assignment of Risk–by Industry[38]

Industries	Risks are assigned exclusively to Audit Committee	Risks are assigned to Audit and other committee(s) not identified as risk committee(s)	Risks assigned to Audit and other committee(s) identified as risk committee(s)	Risk not assigned to committee	Risks assigned to partnered Audit Committee without risk in committee title	Risks assigned to partnered Audit Committee with risk in committee title
Wholesale and Retail (17 companies)	1. Wal-Mart 2. Home Depot 3. McKesson 4. Kroger 5. Target 6. Albertson's 7. Walgreen 8. Lowe's 9. Safeway 10. CVS 11. JC Penny 12. Ingram Micro	1. Sears, Roebuck (Audit, Finance) 2. Sysco (Audit, Finance) 3. Best Buy (Audit, HR, Compensation)		1. Costco	1. Amerisource-Bergen (Audit & Corporate Responsibility Committee)	
Manufacturing (29 companies)	1. Exxon 2. GM 3. GE 4. Chevron 5. Conoco-Phillips 6. Johnson & Johnson 7. Marathon Oil 8. Lockheed Martin 9. Caterpillar 10. Northrop Grumman 11. Delphi 12. Du Pont 13. Int. Paper Co. 14. Honeywell 15. Alcoa 16. Sunoco 17. Merck 18. Bristol-Myers Squibb 19. Abbott Labs 20. Halliburton	1. Ford (Audit, Finance) 2. Valero (Audit, Finance) 3. Pfizer (Audit, Science & Tech) 4. Boeing (Audit, Finance) 5. Procter & Gamble (Audit, Finance) 6. Dow Chem. (Audit, Finance) 7. United Technologies (Audit, Finance) 8. Johnson Controls (Audit, Pension & Benefits) 9. Weyerhaeuser (Audit, Finance)				
Electronics Manufacturing (6 companies)	1. IBM 2. Hewlett-Packard 3. Intel	1. Dell (Audit, Finance) 2. Motorola (Audit, Legal) 3. Cisco (Audit, Finance & Investments)				
Services (8 companies)	1. Cardinal health 2. Altria 3. Medco 4. Caremark Rx 5. Electronic Data Sys 6. WellPoint	1. Microsoft (Audit, Finance) 2. HCA (Audit, Finance & Investments)				
Transportation (3 companies)	1. UPS 2. FedEx 3. Plains All American Pipeline					

Appendix III (continued)

Industries	Risks are assigned exclusively to Audit Committee	Risks are assigned to Audit and other committee(s) not identified as risk committee(s)	Risks assigned to Audit and other committee(s) identified as risk committee(s)	Risk not assigned to committee	Risks assigned to partnered Audit Committee without risk in committee title	Risks assigned to partnered Audit Committee with risk in committee title
Telecommunication (6 companies)	1. Verizon 2. SBC 3. AT&T 4. Sprint Nextel		1. MCI (Audit, Risk Management)	1. BellSouth		
Media (5 companies)	1. Disney 2. Viacom 3. News Corp.	1. Time Warner (Audit, Finance) 2. Comcast (Audit, Nominating & Corporate Governance)				
Food, Beverage & Tobacco (4 companies)	1. PepsiCo 2. Tyson 3. Coca-Cola			1. Archer-Daniels-Midland		
Utilities (1 company)			1. Duke Energy (Audit, Finance & Risk Mgmt.			
Banking (5 companies)		1. Bank of America (Audit, Asset Quality Review) 2. Wells Fargo (Audit, Finance)	1. JP Morgan (Audit, Risk Policy) 2. Wachovia (Audit, Risk)			1. Citigroup (Audit, & Risk Mgmt.)
Diversified Financials (6 companies)	1. Morgan Stanley 2. Merrill Lynch 3. Goldman Sachs 4. American Express 5. Prudential 6. Lehman Brothers					
Insurance (10 companies)	1. AIG 2. Berkshire Hathaway 3. State Farm 4. Allstate 5. Hartford Financial 6. Nationwide	1. MetLife (Audit, Corporate Governance) 2. UnitedHealth Group (Audit, Compliance & Govt. Affairs)	1. St. Paul's (Audit, Investment & Capital Markets, Risk)		1. TIAA & CREF (Audit, Funds Audit)	

36 Prepared by Katharine Rose Newman, The Conference Board.

37 Companies in chart are listed in descending ranking order.

38 Industries with fewer than 5 companies may not be statistically significant. Industries are grouped by The Conference Board and cross-referenced with Forbes.com

The Conference Board Governance Center

Founded in 1993, the Governance Center helps corporations improve their governance processes, inspire public confidence, and facilitate capital formation. In small groups, we bring together corporate executives from leading companies with influential institutional investors. This unique, non-adversarial setting fosters a free-flowing exchange of ideas and concerns.

The Conference Board Directors' Institute

Draws on The Conference Board's decade-long reputation as an impartial and authoritative source of corporate governance best practices. It was launched in response to corporate directors' need for a non-academic, impartial forum for open dialogue about the real-world business challenges they face. Practical, time-efficient programs ensure corporate directors stay abreast of trends in governance and meet the challenges of their unprecedented responsibility and accountability.

Additional Resources

A sample of related offerings from The Conference Board includes:

Councils

Chief Audit Executives
Chief EH&S Officers
Chief Financial Officers
Chief Information Officers
Chief Legal Officers
Chief Privacy Officers
Compensation
Contributions
Corporate Compliance
Corporate Security Executives
Council of Division Leaders - Financial Executives
Council of Division Leaders - Human Resources
Global Council on Business Conduct
Purchasing and Supply Leadership
Senior International Attorneys
Strategic Risk Management
European Council on Corporate Governance and Board Effectiveness

Workshops and Forums

Audit Committee Issues: Workshops for Executives

Corporate Governance and Compliance: A Two-Day "Crash Course"

Corporate Governance Executives Workshop

Webcasts

Conferences

Global Corporate Citizenship and Risk Assessment

Business and Sustainability

Business Ethics

Enterprise Risk Management

Global Leadership Development

For more information about these and other governance opportunities The Conference Board offers, visit **www.conference-board.org/knowledge/governance.cfm**

RELATED PUBLICATIONS FROM THE CONFERENCE BOARD

Research Reports

Revisiting Stock Market Short-Termism
Research Report R-1386-06-RR

Director' Compensation and Board Practices in 2005
Research Report R-1379-05-RR, 2005

Expanding the Investment Frontier: Factoring Environmental, Social and Governance Criteria into Investment Analysis
Research Report R-1378-05-RR, 2005

Institutional Investment Report 2005 U.S. and International Trends
Research Report R-1376-05-RR

The 2005 Top Executive Compensation Report
Research Report R-1377-05-RR, 2005.

Corporate Governance Best Practices in Europe
Research Report R-1375-05-RR, 2005

Corporate Governance Handbook 2005: Developments in Best Practices, Compliance, and Legal Standards
SR-05-02, 2005

The Future of the Annual General Meeting
SR-04-02, 2004

Improving Communications Between Companies and Investors
SR-04-01, 2004

Research Director
Dr. Carolyn Kay Brancato

Publishing Director **Chuck Mitchell**

Authors **Dr. Carolyn Kay Brancato, Dr. Matteo Tonello, Ellen Hexter, Katharine Rose Newman**

Design **Peter Drubin**

Production **Andrew Ashwell**

The Conference Board, Inc.
845 Third Avenue
New York, NY 10022-6679
United States
Tel +1 212 759 0900
Fax +1 212 980 7014
www.conference-board.org

The Conference Board Europe
Chaussée de La Hulpe 130, box 11
B-1000 Brussels
Belgium
Tel + 32 2 675 5405
Fax + 32 2 675 0395
www.conference-board.org/europe.htm

The Conference Board Asia-Pacific
2502C Admiralty Centre, Tower 1
18 Harcourt Road
Hong Kong SAR
Tel + 852 2804 1000
Fax + 852 2869 1403

The Conference Board of Canada
255 Smyth Road
Ottawa, Ontario K1H 8M7
Canada
Tel +1 613 526 3280
Fax + 613 526 4857
www.conferenceboard.ca

ISBN No. 0-8237-0878-0