NACD
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

REPORT OF THE NACD BLUE RIBBON COMMISSION

Risk Governance: Balancing Risk and Reward

PUBLISHED BY

National Association of Corporate Directors

SPONSORED BY

The Center for Board Leadership

AND ITS ALLIANCE PARTNERS

Heidrick & Struggles International, Inc.
KPMG's Audit Committee Institute
Oliver Wyman
Pearl Meyer & Partners
Tatum, LLC
Weil, Gotshal & Manges LLP

National Association of Corporate Directors
2001 Pennsylvania Ave. NW, Suite 500
Washington DC 20006
202-775-0509
NACDonline.org

NACD
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward

A Publication of the
The National Association of Corporate Directors

and
The Center for Board Leadership and its Alliance Partners

Heidrick & Struggles International, Inc.
KPMG's Audit Committee Institute
Oliver Wyman
Pearl Meyer & Partners
Tatum, LLC
Weil, Gotshal & Manges LLP

NACD

Table of Contents

Co-Chairs and List of Commissioners iii

About the Publisher and Sponsors v

Letter from the Co-Chairs 1

Overview and Recommendations 2

Chapter 1: Risk and the Board's Oversight Objectives 4

Chapter 2: Understanding the Critical Link Between Strategy and Risk 6

Chapter 3: The Role of the Board and Its Standing Committees 8

Chapter 4: Ten Principles of Effective Risk Oversight 14

Conclusion 20

Appendices 21

Additional Resources 41

Endnotes 42

LIST OF COMMISSIONERS
With Primary Affiliations and Representative *Board Seats*

Co-Chairs

Reatha Clark King, PhD
General Mills Foundation,
Former President and Chair
Exxon Mobil Corporation;
Lenox Group Inc.

William J. Fallon,
Admiral, U.S. Navy (Ret.)
Neural IQ Government Systems
Tilwell Petroleum, LLC

Commissioners

Dennis Beresford
The University of Georgia
Fannie Mae; Kimberly-Clark Corporation;
Legg Mason, Inc.

Alfred R. Berkeley, III
Pipeline Financial Group, Inc.
ACI Worldwide, Inc.;
Johns Hopkins University;
Realpage Inc.

John Castellani
Business Roundtable

Peter Clapman
Governance for Owners, LLP
AARP Mutual Funds; iPass

Theodore Dysart
Heidrick & Struggles
Worcester Polytechnic Institute

Charles Elson
University of Delaware,
Weinberg Center for Corporate Governance
HealthSouth

Cynthia Fornelli
Center for Audit Quality

Holly Gregory
Weil, Gotshal & Manges LLP

The Honorable Barbara Franklin
Barbara Franklin Enterprises
Aetna, Inc.; American Funds;
Dow Chemical Company

Robert Hallagan
Korn/Ferry International
Berkshire Life Insurance Company; Rescare Inc.

Michele Hooper
The Directors' Council
AstraZeneca; PPG Industries, Inc.;
UnitedHealth Group;
Warner Music Group

Cynthia Jamison
Tatum LLC
B&G Foods, Inc.;
Tractor Supply Co.

David Landsittel
Committee of Sponsoring Organizations (COSO)
Burnham Investors' Trust;
Molex, Incorporated

Steven Lazarus
ARCH Venture Partners
Rand Corporation

Mary Pat McCarthy
KPMG's Audit Committee Institute

William McCracken
Computer Associates, Inc.

Ira Millstein
Weil, Gotshal & Manges LLP
Millstein Center for Corporate Governance and Performance at Yale University

David A. Nadler
Vice Chairman
Marsh & McLennan Companies

John Olson
Gibson, Dunn & Crutcher LLP;
Georgetown University Law Center

Michael Oxley
Baker, Hostetler LLP
NASDAQ OMX

Jonathan Sokobin
Office of Risk Assessment
U.S. Securities and Exchange Commission

John Stout
Fredrikson & Byron
St. Thomas University
American Bar Association;
Center for International Private Enterprise; Milestone Growth Fund

David Swinford
Pearl Meyer & Partners

The Honorable E. Norman Veasey
Weil, Gotshal & Manges LLP
Former Chief Justice,
Delaware Supreme Court

William White
Northwestern University
Bell & Howell (Ret.)
Intermatic Incorporated

Karen Hastie Williams
Crowell & Moring
Continental Air; Chubb Inc.;
Gannett Company;
SunTrust Bank; Washington Gas

Alex Wittenberg
Oliver Wyman, Partner

Brian Wolohan
Public Company Accounting Oversight Board (PCAOB)

Ex Officio

Kenneth Daly
NACD

Peter R. Gleason
NACD

Technical Advisor

Oliver Wyman

Acknowledgment

The Commission is grateful to Oliver Wyman, and in particular Lucy Nottingham, for their contributions in research. Thanks also go to Pat Lee and David Brown of KPMG's Audit Committee Institute for their expertise and editorial support. The Commission also thanks the NACD Chapters in the Capital Area, Chicago, Texas TriCities, Southern California, and New York for the valuable risk roundtables they hosted. Finally, the Commission thanks the NACD Research staff members involved in this project: Kurt Groeninger, Kate Iannelli, Alexandra Lajoux, and Suzanne Meyer.

About the Publisher and Sponsors

National Association of Corporate Directors (NACD), an independent nonprofit organization founded in 1977, is the country's only membership organization devoted exclusively to improving corporate board performance. NACD conducts educational programs and standard-setting research, and provides information and guidance on a variety of board governance issues and practices. Membership comprises board members from U.S. and overseas companies ranging from large publicly held corporations to small over-the-counter, closely held, and private firms. With chapters in many major cities providing educational programs and networking opportunities, NACD operates at both a national and local level.

THE CENTER *for* BOARD LEADERSHIP

In response to growing demand for information and guidance on effective board leadership issues, Heidrick & Struggles International joined with NACD to form the Center for Board Leadership. Heidrick & Struggles International is now joined by five other alliance partners to support the activities of the Center for Board Leadership. This organization, which is international in scope, is focused primarily on defining, establishing, and refining "best practices" to enhance board performance. To accomplish this, the Center for Board Leadership engages in substantive research projects on critical board topics and holds CEO and director roundtable discussions to help organizations continuously improve boardroom performance.

Alliance Partners

Heidrick & Struggles International, Inc. (www.heidrick.com) is a leading executive search firm, specializing in chief executive, board of directors, and senior-level management assignments. Contact Ted Dysart at (312) 496-1860.

KPMG's Audit Committee Institute (www.kpmg.com/aci) was established by KPMG in 1999 as a resource for audit committees and senior management. ACI's main mission is to communicate with audit committee members to enhance their awareness of, commitment to, and ability to implement effective committee processes. Contact Caryn P. Bocchino at (201) 505-2012, or ACI at (877) 576-4224.

Oliver Wyman (www.oliverwyman.com) is the leading management consulting firm combining deep industry knowledge with expertise in strategy, operations, risk management, organizational transformation, and leadership development. Oliver Wyman is part of Marsh & McLennan Companies. Contact Alex Wittenberg at (212) 541- 8100.

Pearl Meyer & Partners (www.pearlmeyer.com) is a leading executive compensation consultant to senior management and board compensation committees, creating custom designed executive and board pay programs in support of the goals and strategic plans of each client. Contact David Swinford at (212) 644-2300.

Tatum, LLC (www.tatum.com) is an executive services firm exclusively focused on creating and supporting the office of the CFO. Delivery of services can be full time, part time, or project based, but always include senior-level, hands on operating experience deploying CFO services customized to each situation. Contact Robert Harman at (215) 242-6526.

Weil, Gotshal & Manges LLP (www. weil.com), an international law firm, has been at the forefront of corporate governance developments for more than two decades. Under the leadership of Ira M. Millstein, the corporate governance practice draws from the firm's corporate, securities, litigation, tax, and restructuring practices. Contact Holly J. Gregory at (212) 310-8038.

Letter from the Co-Chairs

Nothing is more fundamental to business—or more vexing to boards—than risk, particularly in the context of strategic decision making. Risk has always been a companion of reward, inherent in assessing opportunities against a company's strengths and weaknesses.

There is clearly an intense focus on risk today. While risk management has been on the radar—if not a priority—for most companies and boards over the past several years, many are asking whether our current system of corporate governance and strategic decision making ensures adequate risk assessment and management.

But risk *management* is only part of the equation. The full solution entails risk *governance*—the focus of this report. The following pages offer practical advice and suggestions to directors on how they might *improve their processes* for overseeing the company's risk management activities.

In many ways, risk management has always been a battle plan to win the last war. In 1933 and 1934, the U.S. federal government responded to the 1929 stock market collapse with securities legislation designed to solve the problems that led to that collapse. Decades later, the 2002 Sarbanes-Oxley Act created mechanisms designed to prevent activities of the kind that occurred at Enron and WorldCom. Similarly, the legislation and regulations proposed in 2009 responded to the problems of 2008. These after-the-fact measures, while important, highlight the need for engaged and informed directors who foster a value-building strategy while appropriately responding to the attendant risks.

Drawing on the experiences and insights of our Blue Ribbon Commission (BRC) members, research from NACD with Oliver Wyman (Appendix F), as well as the thoughtful work and writings of many others in the business and governance arenas, this report:

- considers the objectives of the board's risk oversight activities
- examines the critical link between strategy and risk
- clarifies the board's role in relation to particular categories of risk
- recommends "Ten Principles of Effective Risk Oversight" as guidance for directors.

Clearly no single approach to risk will fit every organization, but we believe that these principles and this report will allow boards to build a more comprehensive risk oversight system tailored to the specific needs of their companies and industries. This report also can provide management with important insights into the needs and expectations of today's boards with respect to risk and other critical areas of governance.

Our hope is that the guidance and principles set forth in this report provide a starting point—or a turning point—for board discussions about risk as we move forward into a daunting, but ultimately promising, future of balancing risk and reward.

Reatha Clark King
William J. Fallon
October 2009

Overview and Recommendations

Boards today are operating in what may be one of the most challenging business environments any generation of directors has ever known.

The forces shaping the business and governance environments present a daunting array of risks for every company and board. Those risks include the economic crisis, the meltdown of the financial system, emerging markets, globalization, technology innovation, demographic shifts, industry consolidations, and regulatory reform.

The speed of change—and the complexity of risk—means the lead-time that companies and boards have available to see approaching opportunities and changes continues to decline, while the expectations of shareholders, regulators, and others continue to climb. Indeed, we have seen a resurgence of shareholder and federal initiatives aimed at wresting power from the board of directors.

As boards cope with ever-fuller agendas, new responsibilities, potential liabilities, and very often too little time and information, meeting the challenges of effective risk oversight is both formidable and paramount. For this reason, the National Association of Corporate Directors (NACD) convened the 2009 Blue Ribbon Commission on Risk Governance, focusing on the board's role in risk oversight.

The members of this Commission shared their years of accumulated experience and knowledge as business executives, government officials, corporate board members, governance experts, risk consultants, and academics engaged in the study of governance.

Nearly a decade ago, the NACD Blue Ribbon Commission on Risk Oversight issued a landmark report (See Appendix G for the Executive Summary of the report) that offered practical guidance to directors on the subject of risk; but while its guidance was and is still sound, the current business and regulatory environment has posed dramatic new challenges. Given the events of 2008-2009, it is clear that a broader view of risk in the context of strategic decision making is needed to help organizations properly engage risk and its consequences—with the aim of restoring public confidence in the role of boards, and in corporate governance.

In this report, the BRC recommends the following ten principles to guide directors in their efforts to provide effective oversight of risk:

1. Understand the company's key drivers of success.
2. Assess the risk in the company's strategy.
3. Define the role of the full board and its stand-

ing committees with regard to risk oversight.
4. Consider whether the company's risk management system—including people and processes—is appropriate and has sufficient resources.
5. Work with management to understand and agree on the types (and format) of risk information the board requires.
6. Encourage a dynamic and constructive risk dialogue between management and the board, including a willingness to challenge assumptions.
7. Closely monitor the potential risks in the company's culture and its incentive structure.
8. Monitor critical alignments—of strategy, risk, controls, compliance, incentives, and people.
9. Consider emerging and interrelated risks: What's around the next corner?
10. Periodically assess the board's risk oversight processes: Do they enable the board to achieve its risk oversight objectives?

Chapter 1
Risk and the Board's Oversight Objectives

When it comes to risk and risk oversight, it's easy to miss the forest for the trees. The board can lose sight of the big picture; risk-taking may yield rewards, and excessive caution may lead to mediocre performance, and even losses.

It is perfectly appropriate—indeed essential—to the health of our economy, and to product innovation and enhancement, for some companies to adopt business models and strategies that have greater risks than others. In successful businesses, however, boards and management work together to define an acceptable level of risk that produces the greatest opportunity for reward. Without risk, there is no reward. True, there may be a need to curb unbridled risk-taking in certain core industries or large companies, but clearly no single solution fits all situations.

Just as corporate America and, indeed, businesses and policymakers worldwide are taking a step back to reassess the state of risk management, every board is well advised to step back and consider its risk oversight objectives.

Defining the Board's Objectives for Oversight

Before considering how the board should oversee the organization's activities to manage risk, it is helpful to consider the goals and objectives of this oversight effort. What should the board seek to accomplish in its oversight role?

It is important to note that "oversight" is used in a broad manner in this report; it incorporates both the monitoring function of directors as well as decision making that involves business judgment.

While risk oversight objectives may vary from company to company, every board should be certain that:

- the risk appetite implicit in the company's business model, strategy, and execution is appropriate
- the expected risks are commensurate with the expected rewards
- management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company's business model and strategy
- the risk management system informs the board of the major risks facing the company
- an appropriate culture of risk-awareness exists throughout the organization
- there is recognition that management of risk is essential to the successful execution of the company's strategy

While individual boards may have other, more specific risk oversight goals, by clarifying these overarching objectives at the outset, a board will be better positioned to determine how to conduct its oversight.

In the chapters that follow, this report considers how boards might achieve their risk oversight objectives. The report first focuses on the critical link between strategy and risk; it then considers the role of the board and its standing committees in relation to specific categories of risk; and it concludes by offering ten principles of effective risk oversight for boards to consider.

Chapter 2
Understanding the Critical Link Between Strategy and Risk

Every business model, business strategy, and business decision involves risk. *Without risk, there is no reward.* This is an obvious but critical point that bears repeating.

Risk is not merely something to be avoided, mitigated, and minimized; risk is integral to strategy and essential for a business to succeed. **Boards should encourage management to pursue prudent risks to generate sustainable corporate performance and value.** As one BRC commissioner noted, "It is perfectly acceptable for a business model to have very significant, inherent risks. Some business models will have greater—perhaps much greater—risks than others." Indeed, an innovative, high-tech start-up company is, by its nature, a riskier proposition than others.

The board's oversight of risk, therefore, should begin with assessing the appropriateness of the company's strategy and the risk that is inherent in that strategy. This includes understanding and agreeing on the amount of risk the organization is willing to accept or retain—its "risk appetite," based on:

- foreseeable risks
- shareholders' expectations
- available capital
- strategic alternatives
- management skills
- possible rewards
- acceptable volatility

The concepts of *risk appetite* and *risk tolerance* are often confused. *Appetite* refers to the amount of risk that the enterprise is willing to take on, while *tolerance* refers to the degree of variance from the level of appetite that the enterprise is willing to accept.

Directors must also consider the structures needed to support business strategies with greater risk appetites. Risk management systems should reflect the degree of risk a company is willing to take. For example, companies taking greater risks should have more robust checks and balances to stay within established tolerances.

Boards need to be clear about (and ultimately approve) the risk appetite that management is endorsing. Higher risk can mean higher return, but also higher volatility of earnings and perhaps even a threat to the enterprise. Importantly, the failure to clarify risk appetite—and to monitor the company's actions relative to that appetite—also poses a risk to the enterprise. It is important for the board to recognize that approving the company's risk appetite is a fundamental strategic decision.

A thorough understanding of a company's strategy and associated risks will not always protect against every risk. Significant threats to an enterprise may manifest as "black swans"—unquantifiable and unforeseeable events often unrelated to a corporate strategy. Protecting a company from these types of events is difficult but not impossible. The board's wisdom and experience alone may not suffice. Companies require options to endure a black swan scenario.

Too often, the strategic engagement of the board boils down to "review and concur," where the only choice the board has is to accept or reject the proposals of management. Real board engagement and assessment of risk requires choices and alternatives. If the board is provided with several strategic alternatives, with management's assessments of different scenarios of risk and return, it can provide more meaningful input and contribute to the decision-making process.

Such involvement in strategy—from thinking and decision making to planning, execution, and monitoring[1]—can provide the board with invaluable first-hand insight into key risks the company is taking. This involvement also allows a better understanding of the calibration or course-correction that may be required later on.

The predicate for successful risk governance is a sound and comprehensive strategic planning process encompassing the external operating environment, existing and anticipated competition, and company strengths and weaknesses.

Importantly, the board's consideration of the strategy/risk dynamic is not an annual or semi-annual activity or event. Rather, it requires an ongoing effort by the board to monitor the shifting industry landscape and understand the impact on the company's strategy, risk profile, and current operations. An ongoing dialogue with management is required to help ensure that the company's strategy remains appropriate, options are considered, adjustments are made, and strategic and operational risks are managed effectively.

In this regard, boards should stay apprised of any emerging and collateral risks that affect a company's strategy or risk profile. These external issues include demographic shifts, climate change, liquidity, and funding issues, as well as issues with vendors, bankers, or customers.

Awareness of the Strategy-Risk Challenge

A number of surveys indicate that directors are keenly aware of—and clearly concerned about—strategy and risk. In one survey, a quarter of directors identified "risk information not linked to the organization's strategic and operational objectives"[2] as a challenge facing their company; in another, they cited risk/crisis oversight and strategic planning/oversight as areas in which they were "less effective," while ranking these issues among the most important to the board.[3]

Chapter 3
The Role of the Board and Its Standing Committees

For a number of years, there has been an ongoing debate about the role of the board versus its standing committees in the oversight of risk. Boards have taken a variety of approaches to suit their needs, depending on their industry, strategy, and governance structure. Some boards have retained primary responsibility for risk oversight at the full board level, while others have delegated responsibility to the audit committee or to a risk committee.

The New York Stock Exchange (NYSE) rules imposing certain risk oversight responsibilities on the audit committee may cause some confusion with respect to risk oversight duties. The NYSE rules require the audit committee, while "not the sole body responsible for risk," to "discuss policies with respect to risk assessment and risk management."[4]

Accordingly, though the audit committee has a responsibility to discuss the guidelines and policies governing the process by which risk assessment and risk management is undertaken, the full board or another board committee may have primary responsibility for risk oversight.

While there is no one-size-fits-all solution, the Commission believes that, as a general rule, **the full board should have primary responsibility for risk oversight, with the board's standing committees supporting the board by addressing the risks inherent in their respective areas of oversight.** It is rare that any one committee—such as the audit committee or a risk committee—would have the time, resources, and expertise to oversee the full range of risks facing a company. Moreover, the critical link between strategy and risk points to the need for the full board—rather than any one committee—to have responsibility for risk.

When boards do charge a single committee, such as a "risk committee" or an "audit and risk committee" with responsibility for risk oversight, the committee can serve as an aggregator and analyst of the various risks seen by the different committees. Furthermore, such a committee can oversee the company's risk management system and processes. But it is important to note that any committee with the word "risk" in its title cannot be the sole overseer of risk. Risk committees should not replace the board's active engagement in risk oversight. (See Appendix E for a sample risk committee charter.)

The Role of the Full Board

As discussed in Chapter 1, the board's oversight objectives include understanding the risk appetite implicit in the company's business

model and strategy.

In considering the board's role (versus the role of its standing committees) in achieving its oversight objectives, it is helpful to identify the risk areas the board handles directly versus those they oversee. (See sidebar for "Areas of Board Responsibility for Risk Oversight.")

While the *full board* likely does not have the time to consider each relevant risk in detail on an ongoing basis, it does have two basic responsibilities:

- To ensure that management has implemented an appropriate system to manage these risks, i.e., to identify, assess, mitigate, monitor, and communicate about these risks.
- To provide effective risk oversight through the board's committee structure and oversight processes.

Beyond these fundamental responsibilities for risk oversight, the full board should concentrate on the broader implications of a strategic direction and allow the committees to focus on specific areas of risk. In doing so, the full board should create dialogue around three critical areas: tolerances, aggregation, and the underlying assumptions in management's strategy.

Tolerances

Part of a board's oversight function is to help corporations stay on course and steer clear of rocks and shoals. Directors must work with management to keep specific new projects, as well as ongoing operations, on an intended path.

Events and systems need to have known stop-points and a method to return to acceptable limits. **Management and the board should work together to establish acceptable levels of**

Areas of Board Responsibility for Risk Oversight

Regardless of industry, organizational strategy, and the unique risks of every organization, the risks and responsibilities facing each board can be broken into the following broad categories:

Governance Risks – Directors are responsible for decisions regarding board leadership and composition, board structure, director selection, CEO selection, and an array of other governance issues critical to the success of the enterprise.

Critical Enterprise Risks – The board needs to be fully engaged to understand the critical risks facing the enterprise, such as technological obsolescence. This may include the top five to ten risks that threaten the company's strategy, business model, or viability—and the status of management's efforts to manage these risks, for which it is responsible.

Board-Approval Risks – The board must approve of decisions regarding major strategic initiatives. Acquisitions, divestitures, major investments, entry into new markets, or new products, etc., require board approval. These may typically be defined in corporate policies.

Business Management Risks – Directors must be knowledgeable of other risks associated with the operations of the business. These risks include day-to-day operations of the business, which the board does not have the time to consider on an individual basis.

Emerging Risks and Non-Traditional Risks – Directors must be knowledgeable about external risks such as demographic shifts, climate change, as well as catastrophic events. Management, however, is responsible for the handling of these risks.

(See Appendix A, Categories of Risk.)

volatility or variance for each business operation, and agree on plans to restore operations to acceptable risk-tolerance levels when these variances are exceeded. When assessing the tolerances for any plan of action, the board can start by asking management two questions:

1. At which point does this operation/these operations cross the line into unacceptable risk?
2. What action, if any, must the company take if the situation reaches that point?

Management should be able to provide answers to these questions and a clear sense of what risks are driving excess volatility. Risk reporting to the board should note where the organization stands in relation to the established tolerance levels. Some risks, however, cannot entirely be quantified. In those cases, management and the board should focus discussion on potential impact and mitigation methods.

Tolerances are established to set unacceptable loss levels and set expectations around corporate performance, but they are not static. Market forces and other changes will alter the tolerance limits set by management and the board. As the tolerances fluctuate with market forces, management must continually aim to perform at newly established tolerance levels. Nevertheless, boards must be consulted and provide consent before management acts to establish a new tolerance level.

Aggregation and Integration

Individual risks are often presented as separate exposures. These exposures are rarely unique; they often intertwine with others, creating a much larger ripple effect. Taken together, the risks create the organization's overall risk profile. The board, acting in an oversight role, is well positioned to consider the interplay among the various risks.

Failing to realize the interrelationship of risks is only one common obstacle to gaining a big picture of enterprise risk. Management and boards may observe little yellow flags but fail to realize that many "little" yellow flags may add up to a "big" red flag. This is particularly challenging for large corporations with multiple business units. In such situations, it can be particularly difficult to identify the total level of risk, given inter- and intra-business risk correlations. A seemingly isolated risk in a single business unit can cause major losses across an entire organization. In a similar example, troubles at a key supplier can have a ripple effect.

Developing a process to understand the aggregate impact of risks to the organization is the role and responsibility of management. **The board should satisfy itself that management has developed a process that is effective and efficient. Additionally, boards must play an important oversight role and supplement this process by identifying how the risks interrelate with each other.** While the actual structure is best left for management to decide, one possible method for dealing with this problem is to appoint a chief risk officer (CRO) whose duties include analyzing the different risks identified by the operational units and presenting an overall assessment to the enterprise. For the board's part in aggregation, risk committees may also be well-suited to this role but each board must decide upon the optimal committee or full board structure that is best suited to the particular corporation.

Executive compensation is a good example of

how the aggregation of risks may play out across an enterprise. Long the target of shareholder attention, executive compensation has a significant impact on corporate risk. Improper compensation structures and short-term incentives have created massive problems for companies. To help minimize this risk, compensation committees may find it helpful to consider corporate strategy and appropriate time horizons for long-term and sustainable business success. Compensation committees may also seek assistance of external advisors/experts for information on proper metrics to incent managers. Regardless of method, directors need to constantly identify these areas of board oversight that have larger effects across a company.

Underlying Assumptions and Strategic Direction

Every forward-looking plan is based on numerous underlying assumptions, often including future trends in the market, technology, and myriad other variables. The board can challenge management to be consciously aware of these assumptions and to support them with credible data. All predictions of the future contain some level of uncertainty, and all attempts to relate future trends to current corporate plans are inherently subjective. The board's role, therefore, is to question the underlying assumptions and strategic choices that management has made. Well-supported reasoning must carry the day. At the same time, boards need not demand detailed proof and demonstrations of every single idea. Often, CEOs are prized—and rightly so—for their instincts, and boards should respect this form of knowledge as well.

Corporate boards play an important role in oversight and in the creation of sustainable corporate wealth. As such, boards attempt to ensure that a company neither reaches too far, nor fails to reach. Directors should have sufficient skepticism while evaluating plans of action or course corrections whether they feel the plan is excessively risky or not. However, they need not oppose a proposed action merely because it incurs risk.

Sometimes, the greatest risk to a company is standing still in a changing world. Indeed, a car in neutral goes nowhere. In expressing their skepticism, directors need not nitpick; they can focus on management's underlying assumptions for the transaction or operation—for example, assumptions that interest rates will remain stable, key employees will remain with the company, and unique advantages will remain unique. (See Appendix B for a list of questions directors may want to ask.) The goal is to encourage management to re-think proposals, compensate for possible unforeseen events or consequences, and communicate effectively with the board.

To accomplish this approach, directors must stay informed. It is difficult to play the role of constructive adviser in unfamiliar territory. Directors should not hesitate to request more information as they challenge assumptions, especially any information to corroborate or challenge the underlying assumptions made by management. Independent consultants to the board are one possible source of information outside of the boardroom. They can be a useful tool to form alternative perspectives.

It is important to note, however, that the use of independent consultants should not be a tool of first resort. **Boards should seek to possess expertise that matches the company's needs.**

Communication and Coordination Among Committees

To help promote effective communication and coordination of the oversight activities of its standing committees, boards are taking a variety of approaches, including:

- **Mapping oversight responsibilities** to clarify the risk oversight responsibilities of each committee.
- **Overlapping committee memberships or informal cross-attendance** at committee meetings to help ensure that knowledge is transferred between committees regularly, particularly when inter-committee coordination is of strategic importance.
- **Holding regular meetings of standing committee chairs** to discuss oversight activities and issues that may be relevant to the oversight responsibilities of multiple committees; and
- **Requiring robust committee reports for the full board** to help keep all directors informed of key risk-related issues.

When the required skill sets are absent, boards should look to their own composition and make adjustments to meet company demands.

The Role of Standing Committees

Boards focus on the "big picture" of risk affecting the company. In contrast, the role of the board's committees is to oversee the management of risks particular to their subject areas and communicate important information about risks to the full board. While the role of the various standing committees for risk oversight will vary from company to company, it is essential that the board clarify these responsibilities.

Clearly, the audit committee has responsibility for financial reporting risks; and, as noted earlier, the NYSE listing standards require the audit committee to discuss risk assessment and risk management policies. The risk oversight roles of the other two "required" board committees (compensation and nominating/governance) are generally straightforward. Compensation committees focus on proper incentives for executives while the nominating/governance committee concentrates on issues arising from board composition.

The question for every board, however, is how to organize its committee structure to ensure proper oversight of other categories of business management risks—e.g., operational, strategic, financial, human resources (HR)/labor, reputational, and hazard risks—that might pose a particular concern for the business.

For example, some boards have formed finance committees to focus on corporate growth (through mergers or acquisitions), financing, and capital investments, and others have formed compliance committees to address critical compliance issues. Many technology companies have formed technology or science committees to review priorities and investments for research and development, since these investments pose a major strategic risk to the business. Examples of other board-level committees include public policy, safety, HR/labor relations, employee benefits/retirement, investor relations, and environmental policy.

Many banks and insurance companies have formed management-level risk committees, whose members often have specific knowledge or expertise about the risks inherent in the operations of these institutions. The use of risk committees at the board level is not necessarily the panacea that many might think. Although shifting

the burden to a risk committee may help the audit committee, it is still not advisable to place all risk oversight in one place. The full board needs to take responsibility for risk. If a risk committee is formed, it should be the aggregator, not the sole committee responsible for risk at the board level. The same applies to the audit committee.

Despite the clear benefits of committees (including the opportunity for increased focus on risks of particular concern to the company), a complex committee structure with numerous standing committees poses its own risk: a fragmented or "balkanized" environment, in which each standing committee is focused on its own area of oversight, with no one, including the full board, having the "big picture" of the company's risks.

The role of the full board is to ensure that it sees the fullest possible picture about the company's risks, and that its committee structure enables appropriate focus on the key risks to the business.

Chapter 4
Ten Principles of Effective Risk Oversight

The BRC recommends ten principles to help boards strengthen their oversight of the company's risk management system and activities. While oversight practices that work well for one board may not be ideal for another—especially when corporate strategy, culture, and risk profile vary so significantly from company to company—this Commission believes that these principles provide a foundation that boards can use to build a more comprehensive risk oversight system tailored to the specific needs of their respective companies.

1. Understand the company's key drivers of success. Effective oversight of risk, including constructive discussions with management about risk, cannot take place unless directors have a solid understanding of the company's business and industry, and are diligent in staying abreast of the issues and developments affecting the company.

Clearly, management plays a key role in educating directors about the business and industry, as well as the critical issues and risks facing the company, and boards need to set clear expectations for management in this regard. This education should include an adequate process for on-boarding new directors to bring their knowledge of the company up to speed.

But beyond that, directors should take time to "kick the tires" of the business by visiting business locations—including foreign offices—and by meeting with local business unit leaders, employees, and auditors to gain deeper insight into the business. Directors should also find the time to read extensively about the business, the industry, and the competition. Some directors find it helpful to read reports from the analyst community—both buy- and sell-side reports—about the company and its competitors, as well as SEC filings of competitors.

Understanding the business—particularly in the case of directors who do not have prior industry experience—is a significant, often time-consuming undertaking. But it is the foundation for effective oversight of risk and strategy, and the basis for fulfilling the director's role as adviser to management.

2. Assess the risk in the company's strategy. As discussed in Chapter 2, the board's oversight of risk should begin with assessing the appropriateness of the company's strategy and the risk that is inherent in that strategy. This includes understanding and agreeing on the amount of risk the organization is willing to accept or retain—its risk appetite.

3. Define the role of the full board and its

standing committees with regard to risk oversight. As discussed in Chapter 3, while there is no one-size-fits-all solution, the Commission believes that, as a general rule, the full board should have primary responsibility for risk oversight, with the board's standing committees supporting the board by addressing the risks inherent in their respective areas of oversight.

4. Consider whether the company's risk management system—including people and processes—is appropriate and has sufficient resources. Effective risk management requires a system of interrelated parts. While different companies approach this in different ways, the process generally consists of several activities: identifying the company's primary risks; assessing the potential severity, probability, timing, and costs of their impact; applying a strategy to avoid, manage, or mitigate the risks; monitoring the risks; and communicating about the risks throughout the enterprise.

To gain a better understanding of the risk management process, the board may want to have management explain the following issues:

- How will risk be measured—qualitatively, quantitatively, or both ways?
- What measures and methodologies will be used to assess the risk?
- How will risk analysis and reporting information be used during strategic planning?
- How will risk be integrated into financial and strategic management processes?
- How will risk be monitored?
- How will management communicate risk and risk management to stakeholders?

Too often, risk management systems and processes are viewed as a side activity—running parallel to the actual management of the enterprise. It is critical, however, for the systems and processes to be integrated into the management of the business at the enterprise level and embedded across all business units and functions.

Increasingly, companies are naming a CRO, or an equivalent, to provide senior-level leadership and support for risk management, to educate managers throughout the organization, and to provide necessary tools and techniques to support and facilitate effective risk management throughout the enterprise. The CRO is not responsible for managing specific risks; the CRO is responsible for managing the risk management process—and is in a unique position to support the board in its risk oversight efforts.

There is a tendency for boards to focus exclusively on the formal processes for risk identification and quantification; but there is a broader set of issues that may determine a company's effectiveness in recognizing and managing risks and returns. These include strategy, structures and processes, incentives, management and board succession, culture, and leadership. All of these contribute to the company's capacity to effectively manage risk, and the board should monitor how all of these elements come together to create an effective (or ineffective) risk management system.

5. Work with management to understand and agree on the types (and format) of risk information the board requires. Many directors express concern that the quality, and even quantity, of the information they receive about risk hinders their oversight efforts, and as evidenced by the literature on the topic, their concerns are well-founded:

"[T]he board's ability to provide meaningful

oversight and useful advice is determined by the quality, timeliness, and credibility of the information it has. And it's clear to us that most boards have a long way to go in this area."[5]

To address this concern, it is important that boards set aside time at every meeting to discuss with management the critical risk information the board requires and the format in which it is delivered. Boards should also allocate time in their annual calendars for a "deep dive" on various, critical risk areas.

What information does the board require about each of the enterprise risks facing the company as well as the various categories of business management risks? The CRO (or equivalent role) can be useful in helping the board answer this question. Generally, information should cover a broad range of risks, including threats to the enterprise and threats originating with the board's governance decisions. (See Appendix A for more information regarding categories of risk.)

"There is too much information. We spend too much time looking at things that are okay. We need to figure out how to concentrate on what is really important."

–BRC Commissioner

The board should also consider the format or template of the information. Directors often suffer from "information overload" and require shorter, concise presentations to separate what is actionable from what is not. The use of graphs, heat maps, or other visualizations that show probability, impact, and how different assumptions affect forecasts ("what-if?" scenarios) are valuable formats to make information clear and meaningful.[6] (See Appendix D for examples of other information formats.)

"When I first joined the board, a third of the charts I received were a mystery, another third I think I understood, and another third were clear. When I questioned the meaning of the charts, I found that other directors had the same concerns."

—BRC Commissioner

Risk-information flow is a concern for many boards, as the information they receive may come largely from a single source: management. To avoid "asymmetric" information flow, boards should, as a matter of routine, obtain the input of internal and external auditors, as well as the company's legal counsel, regarding management's risk perceptions and assumptions. Periodically, the board should also solicit the views of shareholders. In general, the less evidence management has to support its position, and the more critical the risk, the greater the need for third-party input.

6. Encourage a dynamic and constructive risk dialogue between management and the board, including a willingness to challenge assumptions. An important question for every board is whether it has an engaged culture: "Engaged cultures are characterized by candor and a willingness to challenge."[7]

Business leaders today understand that we have reached an inflection point for corporate governance. Management and the board act as a team, yet, as mentioned earlier, effective oversight requires that directors understand and test management's strategic assumptions, as well as

its core risk assumptions and assessments. An open, participatory culture is essential.

An effective boardroom culture requires directors to come prepared for board meetings (having reviewed the pre-meeting materials). The board's agenda limits presentation time, maximizes discussion time, and focuses on important issues. Board members should be candid, yet constructive in their opinions—willing to challenge management and seek out the views and opinions of other directors. There also should be opportunities for informal interaction among directors.

It is important to recognize that a herd mentality poses an ongoing threat to effective dialogue around risk, or any boardroom topic. Often described as "group-think," this dialogue-killer is frequently the source of undeveloped plans and strategies. Directors do a disservice to management and the company as a whole when they fail to ask questions that they believe may be inappropriate or even simplistic.

Open dialogue also requires that the right people participate in boardroom discussions on risk, including the CEO, COO, CFO, CRO, CIO, the general counsel, auditors, and business unit leaders responsible for managing risks.

Given the importance of board culture, this issue should be at the top of the list when the board conducts its annual self-evaluation.

7. Closely monitor the potential risks in the company's culture and its incentive structure. Among the most critical risks facing any organization today are the risks posed by its tone at the top, culture, and incentive structure. Indeed, these risks, if unattended, may pose the greatest risk of all to the company.

Directors are in a unique position to monitor these risks and to take prompt action when required. The following are among the questions directors should consider:

- What is the style of management? How do they get things done?
- Are open and candid communications encouraged?
- Does management use directors as sounding boards to test assumptions, or as rubber stamps?
- Is there an effective process to facilitate information flow?
- Are incentive compensation targets realistic and focused on the long term? What risks does the incentive structure pose to the enterprise?
- Is there a commitment to competence throughout the organization?
- How does senior management demonstrate its commitment to an appropriate corporate culture?
- Are reputational issues considered in strategic planning?

The Importance of Reputation

Reputational risk can be understood as the risk of loss from any events arising in the conduct of business which damage any stakeholders' perception of the organization or brand. Organizations which have experienced reputational impact—from production delays, rogue employees, corruption issues, or significant business interruption events—often experience market value adjustments, public backlash, and unplanned changes in management. Such reputational risks need to be considered if the business decision moves forward, even if it is legal, potentially profitable, and with little economic downside.

Setting a proper corporate culture also requires transparency, not only between the board and management but also between the company and its shareholders. As shareholder involvement grows, the need for articulating specific structures is becoming necessary, particularly within risk management. To facilitate proper transparency, **directors need to take an active lead and disclose the board's risk management methods and structures to their shareholders.** Disclosures could include which committees oversee which aspects of risk, and how. The board may also choose to disclose how it has assessed its risk appetite and tolerance levels.

8. Monitor critical alignments—of strategy, risk, controls, compliance, incentives, and people. Understanding and strengthening these critical alignments is essential to the successful execution of strategy. In a time of unprecedented economic upheaval, adjusting strategies and restructuring operations can be a formidable challenge. Much can go wrong between strategy formulation and execution. Small deviations may build up over time, and the risk of misalignment may pose a serious risk to the enterprise.

Any significant change—in people, processes, technology, products, key relationships, or strategy—creates risk, and the more complex the change, the greater the risk. Given the speed of change that companies are experiencing today, boards need to test the company's critical alignments on a regular basis. An important question is whether management has a process to identify and link changes and associated risks to the company's risk management, internal controls, compliance, and incentive processes—i.e., to "connect the dots" between the critical alignments.

9. Consider emerging and interrelated risks: What's around the next corner? Beyond current strategic decisions, the board needs to look forward to understand elements in the environment—macroeconomic, political, technological, demographic, climatic/environmental—that may impact the conduct and effectiveness of the business in the future. In fact, the board may be able to provide a unique, value-added perspective because it is inherently less insular than a management team that might be focused on the issue. In addition, directors need to be aware of how the various units of a company interrelate with each other and with outside parties such as key suppliers.

Resilience is an important issue for many companies today, and boards need to be satisfied that their company has appropriate business continuity plans.

Finally, an important risk that every board needs to consider is "management risk," or the risk that management will be unable or unwilling to perform and execute the strategy agreed to by the board.

10. Periodically assess the board's risk oversight processes: Do they enable the board to achieve its risk oversight objectives? Just as the board must monitor and test the effectiveness of management's system for managing risk, the board must also look closely at its own processes and capabilities to oversee risk. A good starting point is to consider whether the processes have enabled the board to achieve the risk objectives it has set for itself (as discussed in Chapter 1). The following are key questions directors might ask themselves:

- Do our discussions reveal the extent of risk the company is taking?
- Do we have an efficient method to identify top risks to the enterprise?

- Do we have the tools and resources to fulfill our risk responsibilities?
- Are we receiving the necessary board education and training regarding risk?
- Is the company's appetite for risk appropriate considering the strategy?
- Do we have a system to manage risks effectively?
- Do we have systems in place to quantify the upside—as well as the downside—of the risks the company is taking?
- Have we allotted sufficient time for discussion?
- How much does each of the key identified risks contribute to variability in financial performance?

Conclusion

Effective risk governance requires understanding a range of issues, including these three fundamental ones: the risk/reward balance, the board's role in risk oversight, and how boards can fulfill that role.

Understanding the risks in a corporate strategy must be a key objective for any board. While no business can succeed without taking on risk, exposure to excessive risks often has catastrophic impacts. However, what is excessive for one company may be moderate for another. Effective risk oversight allows for new corporate endeavors while curbing activities that may threaten corporate survival. The board's role is to encourage risk-taking while ensuring that systems and processes are in place to alert management to threats to the organization. The role of the board, however, does not stop there.

Fulfilling the risk oversight role requires directors to provide clarity and an outside perspective on management's plans. This responsibility requires directors to step back and assess all levels of a risk management plan. This includes probing the appropriateness of both strategy and the information management provides. It also requires understanding the impact of small risks that can accumulate across an organization.

The topic of risk and the role of the board will continue to be a key area of focus and debate for the foreseeable future, as corporate America and policymakers worldwide seek to improve how companies manage—and capitalize on—risk. As a Commission, we recognize that this is a challenging and long-term undertaking, particularly given the complexity in today's world.

In this report, we have presented ideas that will encourage new approaches for governing the array of risks facing businesses now and in the future. The result will be a better balance of risk and reward. Directors must rise to this challenge of risk governance. The confidence of investors and the functioning of our capital markets depend upon it.

Appendices Index

Appendix A: Categories of Risk 22

Appendix B: 25 Questions Every Director May Wish to Consider 24

Appendix C: Developing a Risk Appetite Statement 26

Appendix D: Risk Reporting Recommendations and Examples 29

Appendix E: Sample Risk Committee Charter Language 34

Appendix F: Research Report from NACD and Oliver Wyman 36

Appendix G: 2002 *Report of the NACD Blue Ribbon Commission on Risk Oversight* — Executive Summary 39

Appendix A
Categories of Risk

While the nature of the information required by the board will vary from company to company and risk to risk, the following are examples of the risk information the board might address for each of the categories of risk:

Governance Risks

Directors are responsible for decisions regarding CEO selection and compensation, board leadership and composition, board structure, and other governance issues. These are critical to the success of the enterprise, and require the board to weigh the risks/rewards associated with alternative courses of action. In making these governance decisions, boards typically rely on their own shared business judgment and knowledge of the business supplemented by information provided by third-party advisers, including search firms, compensation consultants, and legal counsel. Boards should periodically benchmark their approach to these issues by considering best practices employed by other boards in connection with similar governance decisions.

Critical Enterprise Risks

For each of the enterprise risks facing the business, the board requires information that will prepare directors for a vigorous discussion with management about the risk. Management is responsible for handling these risks. While each board should consider its own information requirements, risk information for each enterprise risk might include:

- Probability and impact of the risk, defined in terms of its impact on key strategic goals, as compared to other enterprise risks
- Status of management's risk mitigation efforts
- Changes in probability of reward
- Technological obsolescence
- Changes in overall risk assessment over time
- Core assumptions underlying management's risk assessment
- Interrelationships with other risks, particularly other enterprise risks
- Names and contact information for executives responsible for managing the risk

Board-Approval Risks

When management requests board approval for a strategic initiative—such as an acquisition, divestiture, major capital expenditure, or new product line—directors need to satisfy themselves that approving management's recommendation is appropriate. This involves careful consideration and due diligence, including an analysis of the risks/rewards associated with the action recommended by management.

Boards should recognize that management will have a natural bias toward the option or course of action it is recommending, and the board should accordingly exercise a healthy skepticism in considering management's recommendation.

Business-Management Risks

As discussed in Chapter 3, there are other risks associated with the day-to-day operations of the business, which the board does not have the time to consider on an individual basis. As a result, the board should identify specific *categories* of business-management risks that pose a significant threat to the business, and delegate to an appropriate committee (or the full board) responsibility to oversee a specific category of risk (e.g., financial reporting risks to the audit committee). Management, however, is responsible for handling these risks. Business-management risks include:

- **Reporting Risks** such as overlooking material errors in a prospectus
- **Operational Risks** including risks associated with

internal processes, IT, intellectual property, the supply chain, customer service, obsolescence, manufacturing, and the environment
- **Financial Risks** such as overleveraging the balance sheet
- **Human Resources/Labor Risks** such as the risk of losing a key employee or team without a succession plan
- **Compliance Risks** such as the risk of running afoul of a new complex law
- **Reputational Risks** such as those that threaten brand or public standing

Emerging Risks and Non-Traditional Risks

Directors, as a group, need to understand these risks outside of the scope of the risks listed above. These include external risks such as demographic shifts and climate change, as well as catastrophic events, including risks to the power grid, water supply, public health, and cyberinfrastructure. Management, however, is responsible for handling those risks.

Appendix B
25 Questions Every Director May Wish to Consider

Corporate profitability is driven by taking prudent risks after a well thought-out strategy is developed. Opportunities may be lost if corporate decision makers are unduly risk averse. Maintaining the status quo is a choice, but not always the best one. Companies require strong and effective assessment and management of financial, operational, enterprise, and reputational risk. The entire board of directors has a key role in developing strategy, assessing risk, and overseeing risk management.

In developing corporate strategy and a focus on risk, directors should probe management, advisors, and each other by asking at least the following twenty-five questions (though not necessarily in this order):

1. What are we aiming to accomplish, and how (corporate strategy)?
2. What alternative strategies have been considered/explored?
3. Do the directors receive risk material which adequately distills vast quantities of risk information into prioritized, actionable summaries?
4. Are the risks associated with business units presented to the board in a comprehensive, holistic manner?
5. How do the losses which have occurred compare to the risks which have been identified? Are the losses consistent in magnitude and frequency with what one could expect given the risk profile presented to the board?
6. Can management and the board tie profits, as well as losses, to the presented risk profile?
7. How actively are resources—capital, balance sheet, talent—redeployed? Does the organization consistently, and on a timely basis, feed its winners and starve its losers?
8. What could go wrong or derail our strategy? For example, could multiple problems arise simultaneously or sequentially (the "perfect storm")?
9. Has management been forthcoming about any differences among senior leadership regarding material strategic recommendations and decisions?
10. What assumptions underlie our strategy, and which of those assumptions could change/be wrong?
11. What processes did management use to develop strategy and identify risk?
12. Have we achieved a common understanding of what triggers bring an issue to the board's attention?
13. What capabilities are required to address risks? Where do we have capability gaps?
14. Is there a common understanding among management, the board, and board committees about their respective roles, responsibilities, and accountabilities on strategy and risk oversight?
15. Does the board have a clear understanding of where strategy and risk oversight are delegated and what processes are used within management and among business units?
16. Do the board and committees discuss risk appetite with management?
17. How can this discussion become a part of the board's regular routine?
18. Is the board and are the appropriate committees meeting regularly with a chief risk officer (CRO)?
19. If there is a CRO, has the board ensured that the CRO and general counsel have adequate resources and appropriate reporting lines to bring any changes in material risks to the board's attention?
20. Does the board have the appropriate committee structure for its significant oversight obligations in the risk area?
21. Does the board have sufficient personnel (including advisors) and financial resources in place to enable it to fulfill its risk engagement responsibilities?

22. Has the board adopted a board leadership structure that ensures that the independent directors have a clearly defined leader?
23. Do the board and appropriate committees have access to the information they need to provide oversight in troubled financial times?
24. Has the board and have the appropriate committees reviewed the incentive structure with strategy and risks in mind?
25. Has the board and have the appropriate committees reviewed board composition and director skill sets in relation to up-to-date competencies for oversight of the company's strategy, business lines, and material risks?

NACD

Appendix C
Developing a Risk Appetite Statement[i]

Purpose and Benefits of a Risk Appetite Statement

A risk appetite statement resides at the heart of an effective risk management program and is linked to the organization's overall risk management philosophy and strategic ambition. The objective of developing a clearly articulated risk appetite statement is to explicitly define the level and nature of risk that the organization is willing to take in order to pursue its articulated mission on behalf of its shareholders, subject to constraints imposed by debt holders, regulators, and other stakeholders.

With a risk appetite statement in place, an organization can define specific tolerances around its performance, and in doing so, link its risk management processes to the overall management processes. An effective risk appetite statement should:

- Clearly state the amount and types of risks that the organization is comfortable taking.
- Specify maximum tolerable limits and variability in relative parameters, both qualitative and quantitative, based on stakeholder expectations, constraints, and strategic objectives.
- Be actionable by management so that it has a real effect on the organization's business strategy and risk profile.

Developing a Risk Appetite Statement

The process of developing a risk appetite statement is generally iterative as management and the board consider the existing implicit risk appetite as evidenced in current and historical risk-taking characteristics and existing limits, and then considers the desired risk appetite. The process draws on organizational data, policies, management and board interviews, and external applicable data as outlined in **Illustration 1,** on p. 27.

Many quantitative and qualitative factors are considered in the development of a risk appetite, including strategic parameters, stakeholders, corporate values and reputation, financial parameters, and operational parameters.

Overall, the process outlined above can be executed in a relatively short span of time. However, the analysis and insights needed to operationalize such a framework tends to be much more time intensive. In some instances, the organization may need to implement revised performance measures or develop enhanced reporting processes to implement elements of the risk appetite statement. For example, limits on profit volatility should be monitored using measures of risk-adjusted returns on capital (RAROC).

Common Components

There are no standard or regulated components or formats for a risk appetite statement. In general, risk appetite statements will address aspects relating to the organization's financial tolerances, which are typically measured in quantitative statements, as well as elements relating to the organization's values and culture—which are typically presented in qualitative terms.

An example of common components and methods of definition are presented in **Illustration 2,** on p. 27.

i The materials and examples in this Appendix were provided by Oliver Wyman.

Illustration 1: Key Steps in Developing a Risk Appetite Statement

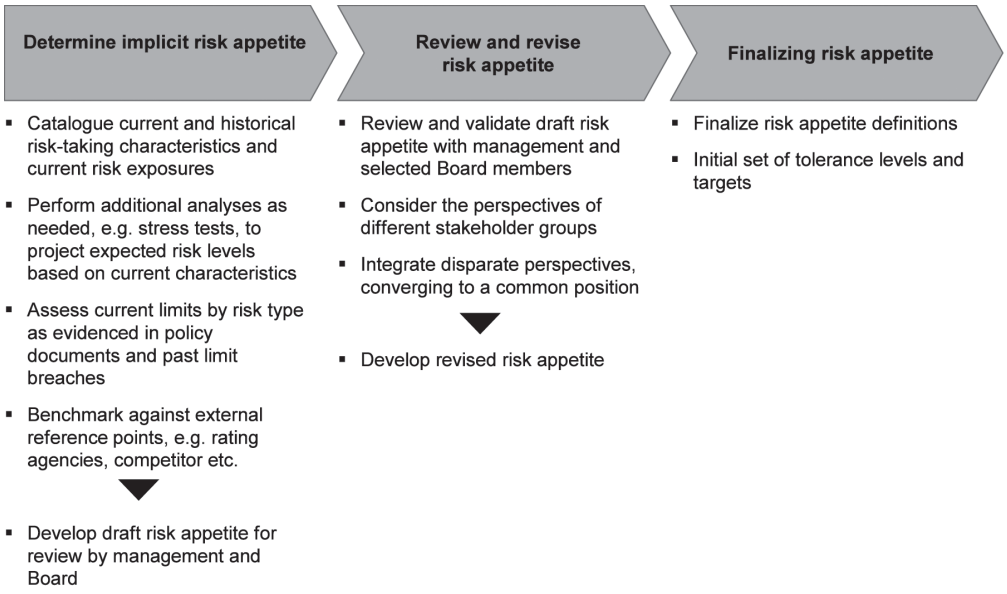


Illustration 2: Sample Risk Appetite Components

	Metric	Illustrative possible components of definition
Quantitative	**Target debt rating**	▪ Define capital requirements ▪ May reference debt ratings set by credit rating agencies
	Earnings volatility	▪ Specify desired earnings forecast by more than X% at a XX% confidence level ▪ Target dividends
	Diversification	▪ Allocation of capital into various business, markets, sectors or clients
	Liquidity headroom	▪ Available liquidity resources to meet requirements at a percentage confidence interval
Qualitative	**Reputation**	▪ Key statements of expected ethical behavior and corporate culture
	Regulation	▪ Statements regarding regulatory compliance
	Governance	▪ Statements regarding organisational governance expectations
	Strategy/growth	▪ Overview of approach regarding risk and strategy / growth expectations

Risk Appetite Statements

Illustrations 3 and **4** are examples of risk appetite statements.

Illustration 3: Risk Appetite Statement from a Financial Services Organization

Criteria	Risk appetite statement
1 Earnings volatility	▪ Deliver annual target EBITDA growth of 15% through 2009 ▪ Maintain a target return volatility of <20% through 2009 (Group level) ▪ Where possible based on liquidity considerations, retain exposure to real estate market volatility
2 Target debt rating	▪ Maintain a target credit rating of AA- (stable) or equivalent across external rating agencies
3 Liquidity headroom	▪ Maintain a target leverage ratio of 55%, with headroom of $600 MM ▪ Review earnings at risk monthly to ensure that potential breach of covenants remains <10% of distribution – Take action in the form of financial products if required to mitigate market risk exposures with a focus on FX and commodities
4 Diversification levels	▪ Limit concentration of large exposures to $2 BN of capital in any one country, $200 MM against any one counterparty ▪ Limit concentration of business unit revenues to 50% of total, and by brand to 5% of total
5 Governance	▪ Ensure operational efficiency and safety standards are maintained within top quartile of industry peer group ▪ Risk retention and coverage levels (property, liability, business interruption) set to limit potential for catastrophic losses at <1%
6 Strategy/ growth	▪ All new business opportunities to be evaluated on a fully-costed, risk-return basis in relation to other investment alternatives ▪ Strategic options to be considered in light of subsequent portfolio diversification implications
7 Regulation	▪ Zero tolerance for any international regulatory breaches ▪ Exceed legal regulatory standards in key geographies
8 Corporate reputation	▪ Maintain a score of >80% on the corporate reputation index (takes into account media, consumer, employee, and analyst views) relative to peer institutions ▪ Ensure external communications adhere to the highest code of legal standards and transparency within all key markets

Illustration 4: Risk Appetite Statement from a Manufacturing Organization

- **Target debt rating:** We will seek to maintain an enterprise-level debt rating of Baa1 – stable
- **Earnings at risk capacity:** We will position ourselves in the top 1/3 of our peer group in terms of deviation from expected earnings.
- **Target capital ratio:** We will seek to maintain a debt to capitalization ratio in the range of 45% - 49%
- **Self-sustaining growth:** New business will not dilute our target capital ratio and we will maintain a working capital ratio between 1.5% – 2.0%
- **Financial strength:** We will maintain an EBIT/ Interest ratio between 5.0% -7.5%
- **Customer dependence:** A single customer will not exceed 15% of total sales
- **Regulatory compliance:** We will seek to score in the top quartile of peer set in regulatory reviews
- **Social responsibility:** We will seek to position ourselves in the top quartile of the ratings of the GRI report

Appendix D
Risk Reporting Recommendations and Examples[ii]

The Purpose of Risk Reporting

Management's regular risk reports to the board should capture and summarize key information to enable the board to provide effective oversight and execute its risk responsibilities as documented in board charters.

There is no single correct format for effective or "right" board risk reports. However, the structure and content of risk reports should align to the following practices to support effective risk oversight:

1. Address the comprehensive range of risks facing the organization as determined by the organization's strategic and operational goals.
   - The report should span the range of material risks that the company has identified as relating to the organization's goals and objectives.

2. Capture and align information at a level that is consistent with the organization's risk management needs and goals.
   - Regular board reports should provide information at a level of detail that is consistent with the director's risk oversight responsibilities and consistent with the level of information determined necessary by the board.
   - Risk exposure data should be presented using metrics that were determined appropriate for that risk type (e.g., qualitative metrics that may be based on a color scheme or quantitative metrics that may include measures such as value at risk).

3. Link risk information to risk appetite and risk tolerances.
   - Board reports should illustrate the organization's risk profile as aligned to its risk appetite statement and link reported risk information to policies for exposure and tolerances.

4. Provide a longitudinal perspective of risk exposures.
   - Current organizational risk exposures or positions should be presented alongside historical data and explanations of trends.
   - Forward-looking trends should be explained in relation to current positions.

5. Update at a frequency consistent with pace of risk evolution and severity of risk.
   - Critical dynamic risk issues can be presented every reporting period.
   - Less dynamic risk issues can be presented on annual basis per a defined schedule.
   - Emerging, material, and threatening risks can be tagged for review at upcoming board meetings.

6. Utilize standardized templates.
   - Templates allow consistent presentation and structure of risk information both between risks and over time.

Risk Report Design

In terms of the actual report design, organizations typically develop a top-line summary report, often called a "dashboard," that enables directors to quickly determine the status of the organization's risk profile and trends as demonstrated by key risk indicators (KRIs).

Beyond the dashboard summary page(s), risk reports can use the following design elements and capabilities to increase effectiveness and "user-friendly" application:

- KRIs marked with "traffic lights" and supported where appropriate by an overview of management plans for risk exposures that are nearing risk tolerances.
  - Risk indicators serve as monitors to help track the organization's risk management performance against set risk tolerances. Traffic light style tagging can help readers quickly determine status

ii The materials and examples in this Appendix were provided by Oliver Wyman.

- Drill-down analysis into risk profiles of different business units and/or specific risk or risk categories.
  - Reports can address the same broad themes as the dashboard but at different levels of detail and focus on a business unit or a risk category

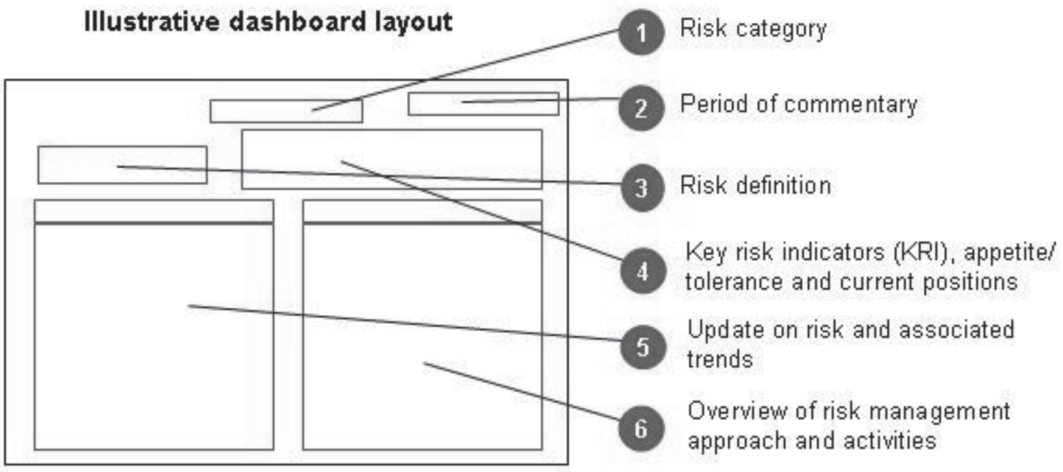
- Value-added commentary plus ad hoc analysis.
  - Tailored analysis that focuses attention on key issues, e.g., relevant trends/threat scenarios or emerging risks

- Appendices.
  - Static or background details on risks (e.g., key definitions, etc.) can be presented in appendices
  - High-level action point tracking (e.g., limit breaches/major risks and follow-up actions)

Risk Report Format Examples

A simple illustrative layout of a risk dashboard is presented in **Illustration 1**, and **Illustrations 2-4** show examples of a risk dashboards developed by corporations.

Illustration 1: Risk Dashboard Layout



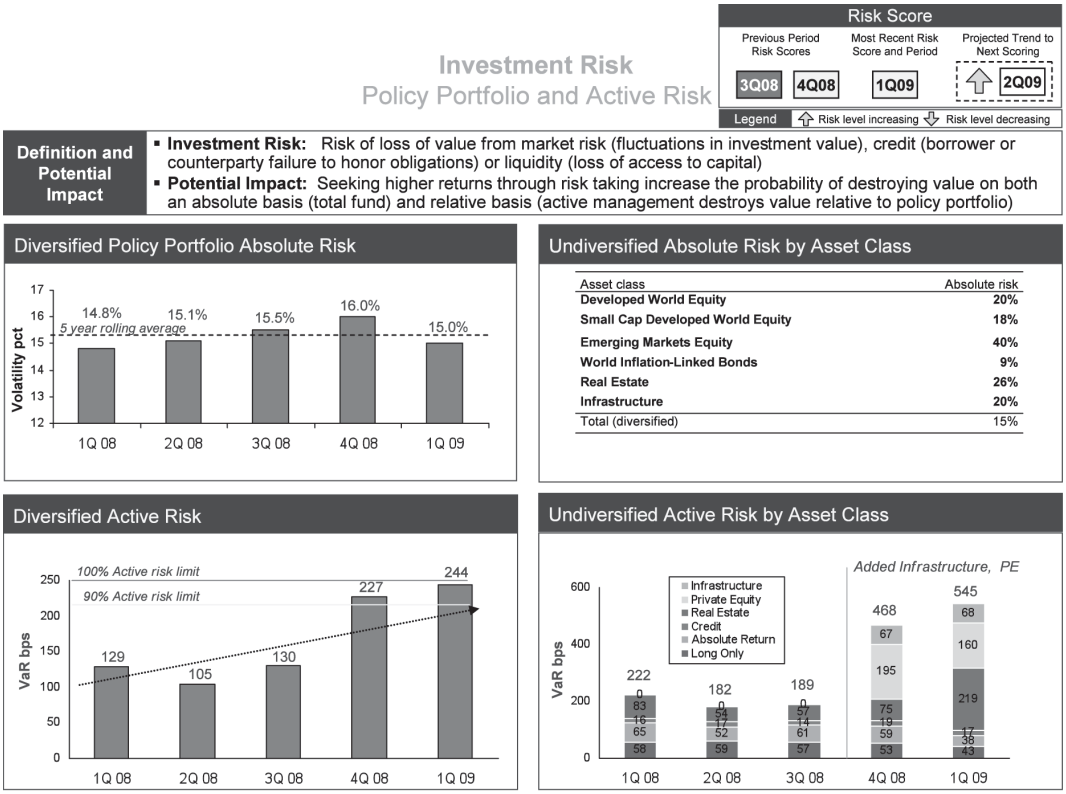
In **Illustration 2**, the dashboard supports drill-down analysis into particular risks.

Illustration 2: Risk Dashboard from a Financial Services Company

	Risk Category	Risk Name	Summary of current exposure and trajectory	Risk Score: Previous Period Scores	Risk Score: Most Recent Score and Period	Risk Score: Projected Trend to Next Scoring
Investment Risk	Investment	Investment (Active)	▪ Increased volatility in private equity and public markets ▪ Increased exposure to RE investments is driving up active risk level ▪ Correlations are increasing in credit related positions and strategies ▪ Risk level likely to increase given larger positions in less liquid investments	3Q08 4Q08	1Q09	↑ 2Q09
		Investment (Policy Portfolio)	Risk level remained stable though asset classes displayed volatility			
Non-Investment Risk	Operational	HR Management/ People	▪ Key vacancy filed, turnover rates returned to expected levels ▪ Exposure to remain stable as turnover remains lower than previous	3Q08 4Q08	1Q09	→ 2Q09
		Information Technology	▪ 1 major IT project completed in period on-time/budget; no IT failures ▪ Exposure likely to increase due to upcoming major IT projects	3Q08 4Q08	1Q09	↑ 2Q09
		Operational/Process Effectiveness	▪ $250K loss due to unwinding of transaction with unapproved party ▪ Exposure to remain stable as policies catch-up to AUM growth	3Q08 4Q08	1Q09	→ 2Q09
	Reputational	Reputation	▪ Press mentions: no negative for Client, 1 negative for external partner ▪ Exposure likely to remain stable as no major events are on horizon	2Q06 2Q07	2Q08	→ 2Q09
	Stakeholder	Regulatory/Government Relationship	▪ No legislation introduced in period directed at the Client ▪ Exposure likely to increase as MP's call for more transparency	1Q08 3Q08	1Q09	↑ 3Q09
	Strategic	Organizational Alignment	▪ Rapid expansion is straining alignment of strategy with org. design ▪ Exposure managed through updated firm vision and initiatives	4Q06 4Q07	4Q08	→ 4Q09

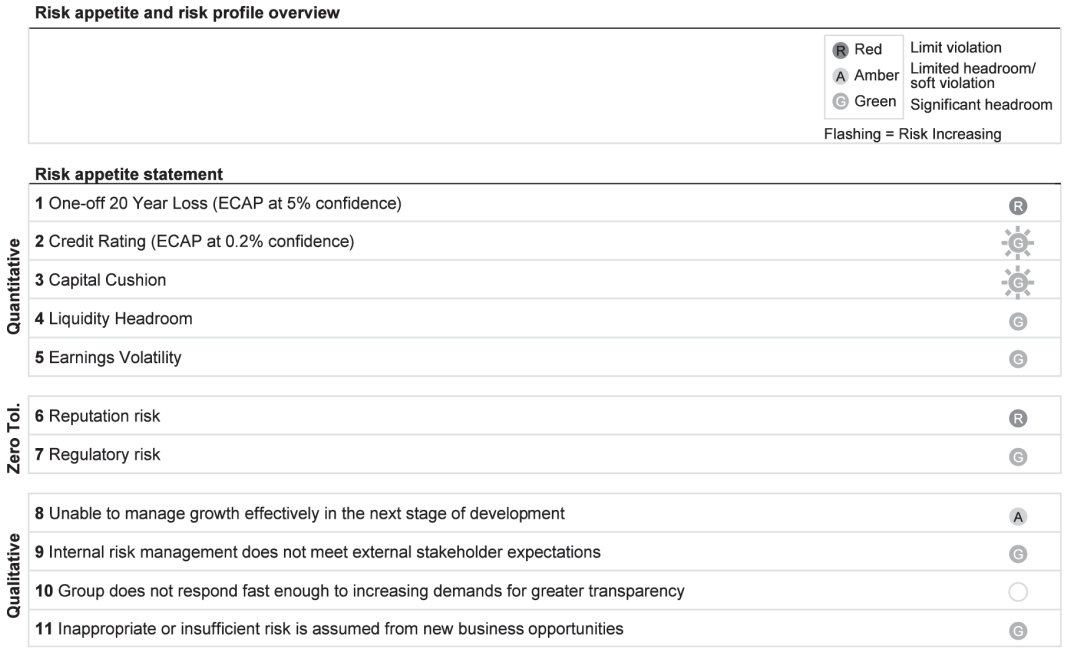
Legend: ↑ Risk level increasing ↓ Risk level decreasing

Illustration 3: Sample Risk Category Drill-Down Report



As noted in **Illustration 3,** it can also be effective to align a page in the board's risk report to the organization's risk appetite statement. An example of such a report structure is provided in **Illustration 4**. As with **Illustration 3,** this overview report can be supported with drill-down reports and data.

Illustration 4: Risk Report Aligned to Risk Appetite



NACD

Appendix E
Sample Risk Committee Charter Language[iii]

I. PURPOSE

To assist the board of directors (the "board") in fulfilling its oversight responsibilities for the risk management oversight and to take or use other means necessary to discharge its responsibilities as described in the company's bylaws and corporate governance guidelines approved by the board.

II. AUTHORITY

The risk committee (the "committee") has authority to conduct or authorize investigations into any matters within its scope of responsibility. It is empowered to:

- Retain outside counsel, accountants, or others to advise the committee or assist in the conduct of an investigation.
- Seek any information it requires from employees—all of whom are directed to cooperate with the committee's request —or external parties so authorized by the committee.
- Meet with company officers, external auditors, or outside counsel, as necessary.

III. COMPOSITION

The risk committee will consist of at least three independent members of the board. A chair shall be elected at the annual meeting of the board from among the committee membership, taking into consideration any recommendations made by the nominating/governance committee in consultation with the lead director.

At least one member of the committee shall have experience in finance or accounting, or other relevant experience or background. All other members of the committee shall be financially literate.

IV. MEETINGS

The committee will meet at least four times a year, with authority to convene additional meetings, as circumstances require. All committee members are expected to attend each meeting, in person or via telephone or video conference. The committee will invite members of management, outside professionals, or others to attend meetings and provide pertinent information, as necessary. It will hold executive sessions attended by committee members only. Meeting agendas will be prepared and provided in advance to members, along with appropriate briefing materials. Minutes will be prepared.

V. RESPONSIBILITIES

The committee will carry out the following responsibilities:

A. Risk Management

1. Monitor all enterprise risks. In doing so, the committee recognizes the responsibilities delegated to other committees by the board and understands that the other committees may emphasize specific risk monitoring through their respective activities.
2. Discuss with management the company's major risk exposures and the steps management has taken to monitor and control such exposures, including the company's risk assessment and risk management policies.
3. Review periodically the activities of the company's risk management committee and all business units, and consider risks that may affect the entire company's viability and the steps taken by management to manage these risks within acceptable tolerances.

iii This Appendix was adapted from a committee charter provided by The Guardian Life Insurance Company of America. The Commission thanks Guardian Life for the permission to use their committee documents. For more information, please see www.guardianlife.com.

B. Reporting Responsibilities

1. Regularly report to the board about committee activities, issues, and related recommendations.
2. Review any other reports the company issues that relate to committee responsibilities.

C. Other Responsibilities

1. Perform other activities related to this charter as requested by the board.
2. Institute and oversee special investigations as needed and receive reports on litigation and fraud.
3. Review and assess the adequacy of the committee's charter annually and recommend changes, if any, to the board for approval.
4. Confirm annually that all responsibilities outlined in this charter have been carried out.

VI. REVIEW OF CHARTER

After initial approval of this charter by the board, the committee shall review periodically the adequacy of this charter and recommend any proposed changes to the board for approval.

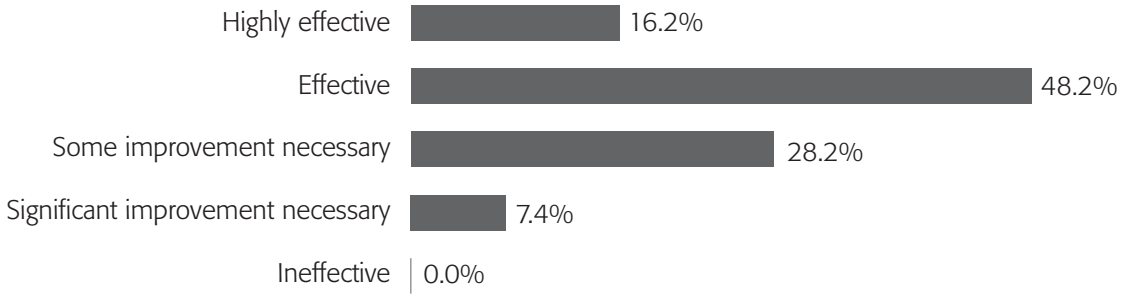
NACD

Appendix F
Research Report from NACD and Oliver Wyman

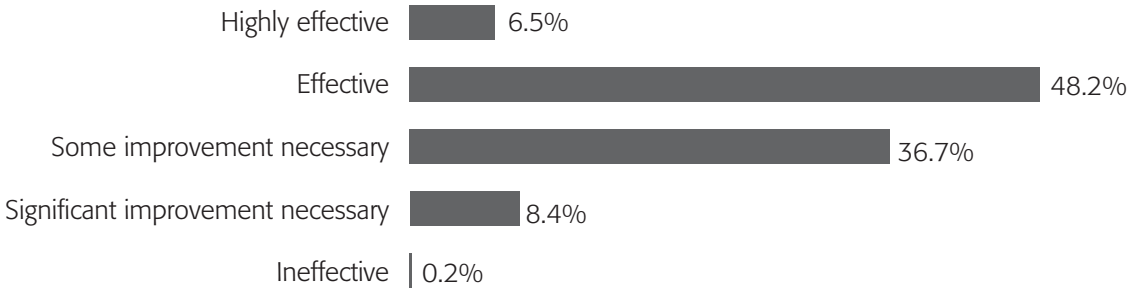
The National Association of Corporate Directors and Oliver Wyman combined resources to study the components of an effective system to oversee a corporation's enterprise risk management. Research was conducted in two parts. The first component consisted of five focus groups in cities across the country: New York, Washington, DC, Atlanta, Los Angeles, and Houston. Approximately 70 directors attended the focus groups. The second component was an online survey of 421 directors conducted during the Fall of 2008 (September 30 through October 8).

Key findings in the survey revealed that most directors are comfortable with the amount of information received from management but they still do not have a complete understanding of how to execute oversight of a risk management program. The survey also showed that directors believe management lacks the ability to define and explain the organization's risk management structure and processes. The data seems to indicate that boards of directors are receiving adequate information about risks and the company but neither the board nor management can fully articulate plans to cope with or mitigate risks. The following are the survey results.

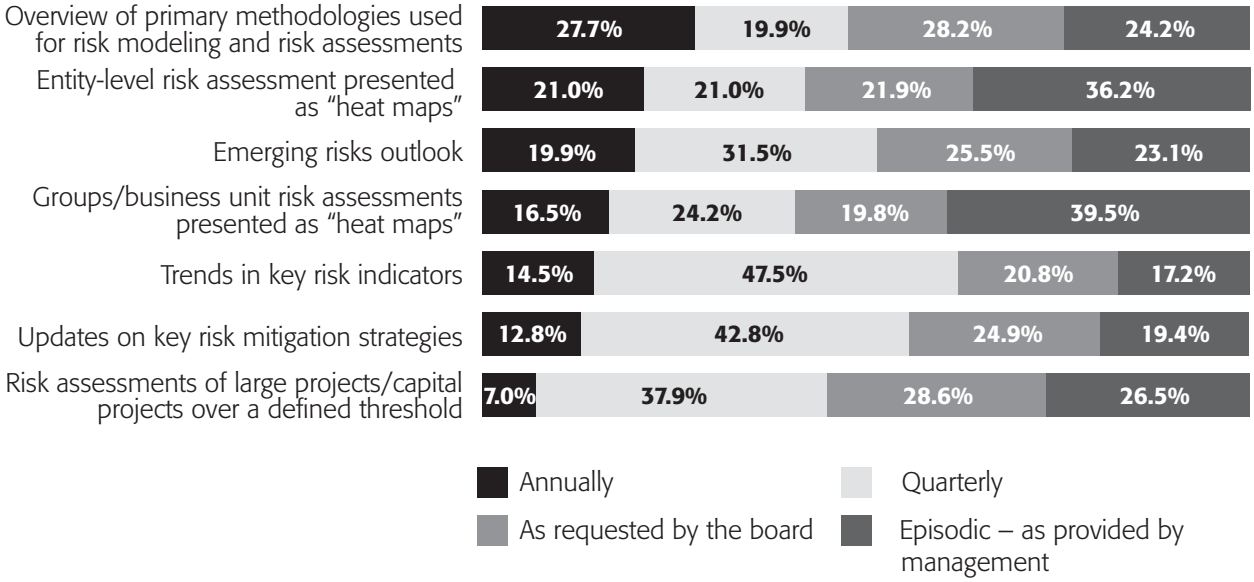
Please rate the board's effectiveness at financial risk oversight



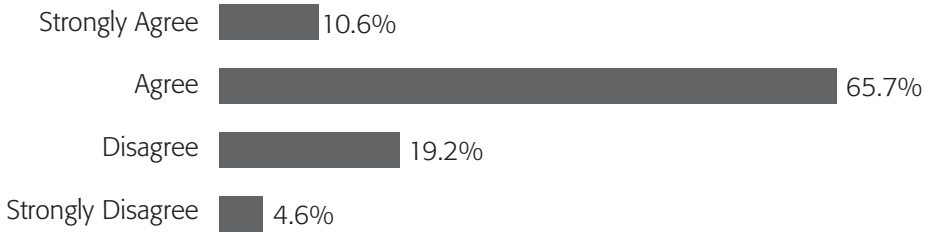
Please rate the board's effectiveness at operational and strategic risk oversight



How often does your board receive the following reports?



Please indicate your agreement with this statement: "Management provides the board with the information necessary to effectively execute its risk oversight."



What are the top three challenges in providing risk oversight?

Who in the organization is responsible for the risk management process?*

*Survey instrument did not include chief information officers as a choice.

Appendix G
2002 *Report of the NACD Blue Ribbon Commission on Risk Oversight*
Executive Summary

Chapter 1: Meeting the Challenge of Turbulent Times through Risk Oversight

- To ensure adequate risk management, directors must understand the specific risks facing the organization they serve, and ensure that there is a process in place to alert them to the occurrence of those risks.
- Directors need to ensure that management has identified the specific material risks the company faces.
- Directors and management should discuss management's plans not only for addressing risks but also for mitigating their impact—minimizing the "spiral factor" of crisis.

Chapter 2: Building a Foundation of Good Corporate Governance

- A foundation of best practices in corporate governance will enable boards to perform risk oversight more effectively.
- If the same person holds both the chairman and CEO positions, then the board should assign the responsibility for ensuring effective board governance to the chairman of a key committee, such as an independent governance committee, or to another independent director.
- As a part of its risk oversight function, the board should work with management to set up a plan that can enable the board to continue to oversee and management to continue to manage during a crisis.
- To ensure the foundation of good governance needed for risk oversight, every board should adopt governance guidelines and every company should have a code of conduct.
- Each director should possess the traits that will serve the company well in the face of change and crisis—including personal integrity, informed judgment, appropriate experience, and financial literacy (or the willingness to acquire it).
- A substantial majority of board members, as well as all members of key committees (audit, compensation, and governance/nominating), should be independent.
- Directors need to identify and eliminate significant conflicts of interest, both for themselves and for the other participants in a corporation's governance and management.

Chapter 3: Overseeing Risk Management

- Directors should ask management to identify and list the principal risks the company faces, indicate the likelihood that they will actually occur, and estimate their potential cost vs. the cost of preventing them.
- The board should ensure that management establishes risk management practices and should continually reevaluate those practices and the board's own role in overseeing them.
- Directors should be "risk-minded" as they review reports, operations, and compliance. Directors should continually monitor and enhance the financial information of the firm, ensuring accurate accounting and safekeeping of corporate assets.
- Directors need to be sensitive to the impact that specific risks may have on each group of stakeholders, including employees, customers, suppliers, and local community groups.
- Directors should provide oversight to help ensure that processes are in place to comply fully with relevant laws and regulations.

Chapter 4: Addressing Specific Risks and Preparing for Crisis

- On a periodic basis, at least annually, the board should review risks and possible "worst-case" scenarios.
- The board can use committees to focus on specific risks. If there is an area of high risk not being covered by a standing committee, directors should consider forming an ad hoc committee to monitor that risk.
- The board should ensure that the corporation has a crisis management plan in place, with a crisis management team to execute and adjust the plan as necessary for a specific crisis.
- The board and management should review crisis management plans on a regular basis, to ensure that they remain relevant.
- The board should designate at least one independent director who would act in times of crisis if management is implicated or otherwise unable to act.

Chapter 5: Responding To and Learning From Crisis

- After a crisis strikes, the company's designated spokesperson (ideally the CEO, but, absent this choice, the chairman or another person in a leadership position) should make a public statement of what happened and what the company is doing about it.
- The company's leadership should have genuine compassion for the victims of the crisis and display that compassion in their words and actions.
- The board should remain informed during a crisis, using a crisis-focused committee if appropriate. In times of crisis, directors should stay on the board, unless they believe that their departure would benefit the company.
- The board's governance/nominating committee should review the board's composition during any critical period to ensure that the board has the capabilities needed to provide effective oversight.
- When a crisis strikes, management and directors should consider engaging appropriate independent advisors, including crisis management specialists, and they should weigh any advice carefully before acting on it.
- Following a crisis, the board should ensure that management conducts an evaluation of risk exposures that led to the crisis as well as the company's response to the crisis. The evaluation should include recommendations for improved practices.

Additional Resources

Aabo, Tom, John R. S. Fraser, and Betty J. Simkins. "The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One." A case study. *Journal of Applied Corporate Finance,* Vol. 17, No. 3. Morgan Stanley. Summer, 2005. Available at http://www.fma.org/.

Apgar, David. *Risk Intelligence: Learning to Manage What We Don't Know.* Boston: Harvard Business School Press, 2006.

Apgar, David. "The Board's Neglected Risk Responsibility," *Directorship.* February/March 2008. Available at http://findarticles.com/p/articles/mi_7521/is_200802/ai_n32263440/.

Auerswald, Phillip and Debra van Opstal. "The Resilience Imperative," *Innovations.* Special Edition for the World Economic Forum Annual Meeting. MIT Press Journal, 2009.

Bernstein, Peter L. *Against the Gods: The Remarkable Story of Risk.* New York: John Wiley & Sons, 1996 and 1998.

Committee on Sponsoring Organizations of the Treadway Commission (COSO). Guidance on Monitoring Internal Control Systems, 2009. Available at http://www.coso.org/GuidanceonMonitoring.htm.

Deloitte LLP, *Perspectives on ERM and The Risk Intelligence Enterprise: Enterprise Risk Management Benchmark Survey.* 2008. Available at http://www.deloitte.com/.

———White Papers: Risk Intelligence Series. 2008. Available at http://www.deloitte.com/.

———*Global Risk Management Survey: Risk Management in the Spotlight,* Sixth Edition. 2009. Available at http://www.deloitte.com.

The Economist. "The World's Best Banks: A Short List." May 21, 2009.

Eggleston, Neil W. and David C. Ware. "Does Your Board Need a Risk Committee?" *Directors & Boards.* Spring, 2009. Available at http://findarticles.com/p/articles/mi_go2446/is_3_33/ai_n31910768/.

"GMI Looks at Corporate Boards and Risk Oversight: Investors Need Greater Transparency." GMI, 2009. Available at www.gmiratings.com.

Hopgood, Suzanne and Michael W. Tankersley. *Board Leadership for the Company in Crisis.* NACD Directors Handbook Series. Washington, 2005. Available at the NACD bookstore, www.nacdonline.org.

National Association of Corporate Directors, *Report of the NACD Blue Ribbon Commission on Risk Oversight: Board Lessons for Turbulent Times.* Washington, DC, 2002. Available at the NACD bookstore, www.nacdonline.org.

National Association of Corporate Directors. White Papers: Series I, Risk Oversight, 2009. Available at https://secure.nacdonline.org/source/members/whitepages/gov-resources.cfm.

National Infrastructure Advisory Council. Risk Management Approaches to Protection: *Final Report and Recommendations by the Council,* October 11, 2005. U.S. Department of Homeland Security. Available at http://www.dhs.gov/xlibrary/assets/niac/NIAC_RMWG_-_2-13-06v9_FINAL.pdf.

Organization for Economic Cooperation and Development. *Corporate Governance and the Financial Crisis: Key Findings and Main Messages.* June 2009. Available at http://www.oecd.org/dataoecd/3/10/43056196.pdf.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable.* New York: Random House, 2007.

Weil, Gotshal & Manges LLP, "Ten Areas for Enhanced Board Focus in 2009, Spotlight on Risk Oversight." 2009. Available at http:www.weil.com.

Endnotes

1 "No More Rubber Stamp: Engaging the Board in Corporate Strategy," David Nadler, *Mercer Management Journal,* May 2007.

2 Oliver Wyman's and NACD's Risk Governance Survey. Conducted between February 17-23, 2008.

3 *2008 NACD Public Company Governance Survey.*

4 Section 303A, NYSE Listing Manual.

5 *Building Better Boards: A Blueprint for Effective Governance,* D. Nadler, B. Behan, and M. Nadler (San Francisco: Jossey-Bass, 2006).

6 "How Boards Can Be Better—a Manifesto," Robert J. Thomas, Michael Schrage, Joshua B. Bellin, and George Marcotte, *MIT Sloan Management Review,* Winter 2009.

7 "Building Better Boards," D. Nadler, *Harvard Business Review,* May 2004.

NATIONAL ASSOCIATION OF
CORPORATE DIRECTORS

1133 21st Street, NW
Suite 700
Washington, DC 20036

PHONE 202.775.0509
FAX 202.775.4857
WEBSITE www.nacdonline.org