Journal of Business & Technology Law

Volume 5 | Issue 1 Article 4

Ignoring the Writing on the Wall: The Role of Enterprise Risk Management in the Economic Crisis

Michelle M. Harner

MICHELLE M. HARNER*

Ignoring the Writing on the Wall: The Role of Enterprise Risk Management in the Economic Crisis

THE RECENT ECONOMIC CRISIS AND GLOBAL RECESSION WERE devastating, but were they really a surprise to those in the financial sector? In January 2005, Federal Reserve Governor Edward Gramlich warned about instability in the subprime mortgage market and possible corrections in the housing market, noting "[t]he subprime incidence of mortgage brokers without a lot at stake in the game is getting pretty high."[1] Likewise, reports indicated that "[r]eal estate gains came to an abrupt halt in the first quarter of 2006, with the median price of a U.S. home falling 3.3 percent from the fourth quarter of 2005."[2] And in February 2006, Washington Mutual cut 2,500 jobs, followed by similar workforce reductions at Lehman Brothers and National City in 2007.[3]

Regulatory agencies and industry organizations also began warning of liquidity issues in the financial markets in late 2006 and early 2007.[4] When asked about these warnings, former Citigroup CEO, Charles Prince, responded: "When the music stops, in terms of liquidity, things will be complicated. But as long as the music is playing, you've got to get up and dance. We're still dancing . . . ."[5] Less than four months after Mr. Prince's statement, Citigroup announced a $6.5 billion write-

* Associate Professor of Law, University of Maryland School of Law. I would like to thank Lisa Fairfax and Joan MacLeod Heminway for their comments on earlier drafts of this essay. I also benefitted from discussions with and feedback from the participants in the University of Maryland School of Law's Roundtable on Corporate Governance, Securities Law and the Financial Crisis. Finally, I thank the University of Maryland School of Law for financial support.

1. Sue Kirchhoff, *Subprime Lending a Worry for Fed Exec*, USA TODAY, Jan. 13, 2005, at 6B.

2. Les Christie, *Real Estate Cools Down*, CNNMONEY.COM, May 16, 2006, http://money.cnn.com/2006/05/15/real_estate/NAR_firstQ2005_home_prices/index.htm.

3. *Washington Mutual to Cut 2,500 Jobs*, N.Y. TIMES, Feb. 16, 2006, at C2; Yalman Onaran & Elizabeth Hester, *Lehman Brothers, National City Cut Jobs as More Home Loans Sour*, BLOOMBERG.COM, Sept. 6, 2007, http://www.bloomberg.com/apps/news?pid=20601087&sid=AYNLkXpO4K3I.

4. *See, e.g.*, Grant Kirkpatrick, *The Corporate Governance Lessons from the Financial Crisis*, FIN. MARKET TRENDS, Feb. 2009, at 4, *available at* http://www.oecd.org/dataoecd/32/1/42229620.pdf.

5. Michiyo Nakamoto & David Wighton, *Citigroup Chief Stays Bullish on Buy-Outs*, FT.COM, July 9, 2007, http://www.ft.com/cms/s/0/80e2987a-2e50-11dc-821c-0000779fd2ac.html.

down and Mr. Prince's resignation.[6] Citigroup, under Mr. Prince's leadership, took a bullish approach to the crisis and firm risk management, and its stakeholders ultimately paid a significant price.

This essay examines the different approaches to enterprise risk management (ERM) adopted by financial institutions affected by the 2008 economic crisis and how ERM contributed to the survival or failure of those firms.[7] It then considers ERM in the broader context of corporate governance generally. This discussion reflects on ERM techniques for corporate boards and whether boards do or should have a duty to implement an effective ERM program. The essay concludes by encouraging boards, stakeholders, and policymakers to give more attention to ERM programs.

ERM AND THE ECONOMIC CRISIS

ERM typically is defined as:

> *[A] process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*[8]

ERM integrates behavioral risk management—e.g., corporate governance—with technical or purely financial risk management, such as financial modeling and stress testing.[9] Although both types of risk management showed significant weaknesses in the 2008 economic crisis, this essay concentrates on the corporate governance aspects of ERM.

---

6. Tomoeh Murakami Tse, *Citigroup CEO Resigns; Former Treasury Chief Named Chairman*, Wash. Post, Nov. 5, 2007, at A16.

7. This essay uses the term "2008 economic crisis" to reference the entire period of financial turmoil, which became widely evident in late 2007 and continued into 2009.

8. Comm. of Sponsoring Orgs. of the Treadway Comm'n (COSO), Enterprise Risk Management—Integrated Framework: Executive Summary 2 (2004), http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf [hereinafter COSO Report].

9. ERM targets overall firm risk strategy and thus includes all types of potential risk impacting firm performance. These risks can be categorized broadly as financial risks; operational risks; business risks; litigation risks; and governance and human resource risks. *See, e.g.*, The Conference Board, The Role of U.S. Corporate Boards in Enterprise Risk Management 11(2006) [hereinafter Conference Board Report]; *see also* Betty Simkins & Steven A. Ramirez, *Enterprise-Wide Risk Management and Corporate Governance*, 39 Loy. U. Chi. L.J. 571, 584 (2008) ("Under ERM, risks can be viewed as falling into two broad areas: core risks (risks which a firm should have a competitive advantage to handle in their business model) and non-core risks (risks which could be hedged by the business or transferred through risk management techniques)."); Martin Lipton et al., Risk Management and the Board of Directors 7–13 (2008), http://blogs.law.harvard.edu/corpgov/files/2008/11/risk-management-and-the-board-of-directors.pdf (identifying thirteen areas of risk that boards should consider in designing and implementing ERM programs).

ERM targets overall corporate strategy and, when implemented correctly, can manage a corporation's risk appetite and exposure. When ignored or underutilized, it can contribute to a corporation's demise.[10] In fact, many commentators point to ERM failures as contributing to the severity of the 2008 economic crisis. As one industry observer stated: "[T]he financial crisis is the result of a failure of risk management [in the banking and securities markets] on a colossal scale. . . . How did so many major financial players miss or overlook such huge, systemic exposures?"[11]

A study by the Senior Supervisors Group also suggests that firms with more integrated ERM programs addressed the issues presented by the crisis in a more efficient and effective manner.[12] The study found that "[f]irms that avoided [significant] problems demonstrated a comprehensive approach to viewing firm-wide exposures and risk, sharing quantitative and qualitative information more efficiently across the firm and engaging in more effective dialogue across the management team."[13] It also identified weaknesses in certain firms' communication and understanding of risk appetite, balance sheet growth, and liquidity needs. For example, risk managers at UBS learned of potential significant subprime losses in early 2007, but senior management did not understand the extent of the losses until July and did not report the issue to the board until August.[14]

The findings of the study and the movement toward more integrated ERM are logical. The earlier a problem is detected and addressed, the more effective the treatment. Boards may not have been able to prevent the crisis itself. Systemic risk frequently is difficult to identify and manage.[15] Nevertheless, boards and senior

---

10. Government officials and commentators alike have recognized the failure of most firms' ERM in connection with the 2008 economic crisis. *See, e.g.*, Ben S. Bernanke, Chairman, Fed. Reserve, Address at the Federal Reserve Bank of Chicago's Annual Conference on Bank Structure and Competition (May 15, 2008), *available at* http://www.federalreserve.gov/newsevents/speech/bernanke20080515a.htm; Roger Barker, *Observations on the Current Crisis from a Corporate Governance Perspective*, Inst. Directors, Feb. 20, 2009, at 2, http://www.iod.com/intershoproot/eCS/Store/en/pdfs/article_responding_crisis.pdf.

11. Risk & Ins. Mgmt. Soc'y, Inc., The 2008 Financial Crisis: A Wake-Up Call for Enterprise Risk Management 3 (Bill Coffin ed., 2009), http://www.RIMS.org/ERMwhitepaper (follow "2008 Financial Crisis a Wake-Up Call for ERM" hyperlink) (quoting Robert P. Hartwig, President of the Insurance Information Institute).

12. *See* Senior Supervisors Group, Observations on Risk Management Practices During the Recent Market Turbulence (2008), http://www.newyorkfed.org/newsevents/news/banking/2008/ssg_risk_mgt_doc_final.pdf. The Senior Supervisors Group represents supervisory agencies from several countries, including the United States, United Kingdom, and France. *Id.* at 22. The study evaluated the risk management practices of eleven major financial institutions involved in the 2008 economic crisis. *Id.* at 1. Although the Senior Supervisor's Group Study focused on financial firms, the same ERM concepts also apply to non-financial firms. Kirkpatrick, *supra* note 4, at 17–18 (discussing ERM in the context of non-financial firms).

13. Kirkpatrick, *supra* note 4, at 8 (summarizing findings of the Senior Supervisors Group Study).

14. *Id.* at 11–12.

15. Systemic risk can be defined as "'the probability that cumulative losses will occur from an event that ignites a series of successive losses along a chain of [financial] institutions or markets comprising . . . a system.'" Steven L. Schwarcz, *Systemic Risk*, 97 Geo. L.J. 193, 196–97 (2008) (quoting Alan Greenspan, Remarks at a Conference on Risk Measurement and Systemic Risk, Bd. of Governors of the Fed. Res. Sys. (Nov. 16, 1995)). Duke Professor Steven Schwarcz has examined various definitions of systemic risk, identifying the

management teams likely could have mitigated losses and the severity of the crisis with more information and a better understanding of their firms' overall financial positions.

But is this type of oversight the board's responsibility? The following discussion considers the appropriate role of the board in ERM and, in turn, the role of ERM in corporate governance.

ERM, THE BOARD, AND CORPORATE GOVERNANCE

Certain key elements of ERM suggest that its implementation is a function of the board.[16] These elements include objective setting, risk assessment, risk response, and communicating and monitoring the firm's overall risk position.[17] The board cannot achieve ERM without the assistance of managers at all levels of the firm. As demonstrated by the 2008 economic crisis, boards cannot, however, completely relegate ERM responsibility to senior or lower management or an already overburdened audit committee.[18]

Several organizations outline a meaningful role for the board in ERM or ERM-like activities. For example, the Principles of Corporate Governance promulgated by the Organisation of Economic Co-operation and Development list the following as board responsibilities: "[r]eviewing and guiding corporate strategy, major plans of action, risk policy, annual budgets and business plans; setting performance objectives; monitoring implementation and corporate performance . . . ."[19] Similarly, the American Law Institute's Principles of Corporate Governance charge the

---

common trait of a triggering event, and has proposed regulations that establish a "liquidity-provider of last resort" to minimize systemic risk. *Id.* at 241–42. In response to the 2008 economic crisis, regulators are rethinking ways to detect and reduce systemic risk. *See, e.g.*, *Financial System Regulation: Hearing Before the H. Comm. on Financial Serv.*, 111th Cong. (2009) (statement of Tim Geithner, Treasury Secretary, U.S. Department of the Treasury), *available at* http://www.treas.gov/press/releases/tg71.htm (suggesting ways to reduce systemic risk, including the creation of a separate entity to monitor risk); Ben S. Bernanke, Chairman, Fed. Reserve, Address at the Council on Foreign Relations (Mar. 10, 2009), *available at* http://www.federalreserve.gov/newsevents/speech/bernanke20090310a.htm (same).

16. Specifically, ERM implicates the board's duty to be informed fully, act in good faith, and implement appropriate oversight procedures. These and other board duties in the context of ERM are discussed below. *See infra* notes 46–61, 65–71 and accompanying text.

17. *See* COSO Report, *supra* note 8, at 3–4. The COSO Report details the components of an integrated ERM program; the roles of the board, senior management, and others in that program; and the importance of prioritizing all types of firm personnel in developing risk-related strategies. *Id.* at 3–4, 6–7.

18. *See* Conference Board Report, *supra* note 9, at 26 (explaining that "[i]n examining the committee charters of the Top 100 Fortune companies, 66 percent of company charters explicitly ascribe risk solely to their audit committee" and commenting that "audit committees, already overburdened, may not have the skills to oversee an enterprise-wide risk management program which would be based on a wider range of issues than financial reporting and controls"); Kirkpatrick, *supra* note 4, at 5–12 (examining ERM structures and their role in the 2008 economic crisis). Notably, Citigroup follows this approach, assigning risk responsibilities at the board level to an Audit and Risk Management Committee. *See* Citigroup Inc., Annual Report (Form 10-K), at 51 (Feb. 27, 2009) [hereinafter Citigroup 10-K 2009] (for the period ending Dec. 31, 2008).

19. Org. of Econ. Co-operation and Dev., OECD Principles of Corporate Governance 24 (2004), *available at* http://www.oecd.org/dataoecd/32/18/31557724.pdf [hereinafter OECD Principles of Corporate Governance].

board to "[o]versee the conduct of the corporation's business to evaluate whether the business is being properly managed . . . [and to review and,] where appropriate, approve the corporation's financial objectives and major corporate plans and actions."[20]

Nevertheless, studies of corporate boards indicate a lax approach or, at best, a general indifference toward ERM.[21] In a survey of senior financial executives, seventy-two percent of the respondents "expressed concern about their own company's risk management practices and ability to meet strategic plans."[22] A survey of board audit committees indicated that only forty-six percent of respondents were very satisfied with their company's process for identifying risk, and only thirty-eight percent were satisfied with the risk reports they received from management.[23]

Perhaps the 2008 economic crisis will encourage boards to reassess their firms' ERM programs. At least one of the surveys discussed above suggests this to be the case.[24] In addition, Standard & Poor's is incorporating the strength of firms' ERM into its ratings calculation.[25] These signs are encouraging. Whether memories of the crisis result in long-term change or simply fade quickly, however, remains to be seen.

ERM BEST PRACTICES: LESSONS FROM THE ECONOMIC CRISIS

As discussed above, UBS's risk management process failed to detect in a timely manner or mitigate the consequences of the 2008 economic crisis. UBS addressed these issues in its 2008 annual report, explaining:

---

20. Principles of Corporate Governance: Analysis & Recommendations § 3.02(a)(2)–(3) (Am. Law Inst. 1992) [hereinafter ALI Principles of Corporate Governance]. The reporter's note to ALI Principles of Corporate Governance also explains that, in determining whether action is within the authority of senior executives or requires board action, parties should consider "the economic magnitude of the action in relation to corporate assets and earnings, the extent of risk involved, the time span of the action's effect, and the cost of reversing the action." *Id.* § 3.01 Reporter's Note. The notes further suggest that board action is required for "actions that would foreseeably expose the corporation to significant litigation or significant new regulatory problems." *Id.*

21. *See, e.g.*, Simkins & Ramirez, *supra* note 9, at 584 ("Evidence from studies and surveys indicates that, to date, only about 10% of major companies claim to have implemented many aspects of ERM, while almost all the others claim that they plan to do so in the future.").

22. Towers Perrin, Financial Crisis Intensifies Interest in Risk Management Among CFOs (2008), http://www.towersperrin.com/tp/showdctmdoc.jsp?url=master_Brand_2/USA/News/Spotlights/2008/Sept/2008_09_30_spotlight_cfo_survey.htm#.

23. *Audit Committees Put Risk Management at the Top of Their Agendas*, KPMG, June 16, 2008, http://www.kpmg.co.uk/news/detail.cfm?pr=3120 (discussing a survey of approximately 1,000 audit committee members from companies around the world conducted between November 2007 and March 2008).

24. *See* Towers Perrin, *supra* note 22 (noting that fifty-five percent of respondents anticipated changes in risk management practices).

25. Standard & Poor's, Enterprise Risk Management: Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings 2 (2008), http://www2.standardandpoors.com/spf/pdf/events/CRTconERM5908.pdf ("[W]e will enhance [the] ratings process for nonfinancial companies through an enterprise risk management (ERM) review.").

> *UBS was severely affected by the financial crisis that unfolded in 2007 and worsened in 2008. UBS entered 2008 with significant legacy risk positions, particularly related to US real estate and other credit positions, which exceeded the firm's risk bearing capacity. As reported during 2008, UBS incurred significant losses on these positions. Risk reduction will remain a priority for UBS until risk exposure is commensurate with the firm's targeted risk appetite. UBS identified significant weaknesses in its risk management and control organization, as well as limitations in its traditional market risk, credit risk, liquidity risk and funding risk measures (including the interplay between these measures). As a result of these weaknesses, the firm failed to adequately assess correlated risks and risk concentrations.*[26]

Prior to the crisis, UBS followed a "silo" approach to risk management.[27] Each group within the organizational structure had a role to play in the risk management process, but there was little coordination, communication, or monitoring among the groups. For example, UBS's Board of Directors was "responsible for the firm's fundamental approach to risk, for approving . . . risk principles and for determining . . . risk capacity."[28] The board had no meaningful involvement, however, in the development, implementation, or monitoring of the process. Those tasks were divided among various groups, including the Executive Board, the Chief Risk Officer, the Chief Financial Officer, and the General Counsel.[29] This silo or segregated approach to risk management was and, to some extent, still is common among financial institutions and other firms.[30] Moreover, many firms, including

---

26. UBS AG, Annual Report (Form 20-F), at 120 (Mar. 11, 2009) (for the period ending Dec. 31, 2008).

27. *See* Thomas L. Barton et al., Making Enterprise Risk Management Pay Off 11 (2002) (distinguishing the silo approach from firm-wide enterprise risk management and discussing the early prevalence of the silo approach); Simkins & Ramirez, *supra* note 9, at 581 (explaining the silo approach as the "management of insurance, foreign exchange risk, operational risk, credit risk, and commodity risks each conducted as narrowly-focused and fragmented activities").

28. UBS AG, Handbook 2006/2007, at 58, http://www.ubs.com/1/e/investors/annualreporting/archive.html?template=layer&selected=125275 (follow the "English" hyperlink in the "Handbook" column and "2006" row) [hereinafter UBS AG Handbook].

29. *Id.* UBS describes its Executive Board as an executive team that includes "the Group CEO, the CEOs of the three Business Groups as well as senior leaders representing major growth businesses and geographic markets" and that is responsible for business management. *See* UBS AG, Annual Review 2006, at 32, http://www.ubs.com/1/e/investors/annualreporting/archive.html (follow the "English" hyperlink in the "Annual Review" column and "2006" row) (explaining the structure and purpose of the Executive Board and the dual board requirement imposed under Swiss banking law).

30. *See, e.g.*, Simkins & Ramirez, *supra* note 9, at 581, 587 (noting that "many organizations still continue to address risk in 'silos'" and explaining that this structure often is a CEO-centric model); *see also* Citigroup Inc., Annual Report (Form 10-K), at 59 (Feb. 23, 2007) ("The independent risk managers at the business level are responsible for establishing and implementing risk management policies and practices within their business, for overseeing the risk in their business, and for responding to the needs and issues of their business."); Goldman Sachs Group Inc., Annual Report (Form 10-K), at 105 (Jan. 27, 2009) ("Segregation of duties and management oversight are fundamental elements of our risk management process."); Goldman Sachs Group Inc., Annual Report (Form 10-K), at 88 (Feb. 6, 2007) (same). Notably, Citigroup revamped its approach to risk management during 2008 and now reports that "[s]ignificant focus has been placed on fostering a risk

UBS, Lehman Brothers, and Wachovia, limited the role of the board in the risk management process.[31]

In response to the crisis, UBS revamped its risk management structure to, among other things, "strengthen the roles and responsibilities" of the board and "integrate its approach to risk control."[32] UBS created a new risk committee of the board to "oversee[ ] the firm's risk profile and the implementation of risk management and control principles."[33] It also increased the emphasis on risk reporting, providing for certain daily reports to senior management and monthly and quarterly reports from the business divisions for purposes of updating the board.[34] Although the value of any ERM program lies primarily in its execution, UBS at least is establishing a viable framework.

Best practices promulgated by industry organizations urge firms to take an integrated approach to ERM. "Cultivation of a consistent 'risk culture' throughout firms is the most important element in risk management."[35] These reports emphasize that risk management cannot be static and is most effective when it is "built into an entity's infrastructure" and "intertwined with an entity's operating activities."[36]

The board can play a key role in developing a firm's ERM and cultivating a risk culture. Some commentators suggest that the board, among other things, "evaluat[e] the risks associated with corporate strategies, defin[e] the risk appetite of the company, [and] ensur[e] that appropriate resources are devoted to risk identification, avoidance, and mitigation."[37] Others urge boards to review and reassess the composition and expertise of risk management committees, clearly define re-

---

culture based on a policy of 'Taking Intelligent Risk with Shared Responsibility, without forsaking Individual Accountability.'" Citigroup 10-K 2009, *supra* note 18, at 51.

31. Lehman Bros. Holding, Inc., Annual Report (Form 10-K), at 69 (Jan. 29, 2009) (board members not included in risk committee); Wachovia Corp., Annual Report (Form 10-K), at 34 (Feb. 28, 2007), *available at* https://www.wachovia.com/common_files/2006_Annual_Report.pdf (explaining that board members are not included in the risk committee; the risk committee reports to the board of directors); *see also supra* notes 27–29 and accompanying text.

32. UBS AG, Annual Report (Form 20-F), at 120 (Mar. 11, 2009) (for the period ending Dec. 31, 2008).

33. *Id.* at 121.

34. *Id.* at 122.

35. Peter Green & Jeremy Jennings-Mares, *IIF's Final Report on Market Best Practices for Financial Institutions and Financial Products*, Banking & Fin. Serv. Pol'y Rep., Sept. 2008, at 1; *see also* Conference Board Report, *supra* note 9, at 23 (quoting Jenne K. Britell, Chairman and CEO, Structured Ventures, Inc. and director of various companies as saying "[w]ithout tone at the top, a company can never have enough auditors, lawyers or compliance to make risk oversight work").

36. COSO Report, *supra* note 8, at 17.

37. Barker, *supra* note 10, at 2; *see also* Contemporary Risk Mgmt. Policy Group, Containing Systemic Risk: The Road to Reform 11–12 (2008), http://www.crmpolicygroup.org/docs/CRMPG-III.pdf [hereinafter CRMPG Report] (recommending "comprehensive exercises aimed at estimating risk appetite" and encouraging involvement of the board and senior management).

sponsibility for risk decisions, and ensure a robust reporting system.[38] To perform any of these tasks, "the boards need to be educated on risk issues and to be given the means to understand risk appetite and the firm's performance against it."[39]

Consequently, communication and coordination among the board, senior management, and others in the firm are essential to effective ERM. These elements also are among the most challenging for large business entities to implement. Some commentators suggest using a Chief Risk Officer (CRO) to facilitate information flow; others suggest forming a risk committee separate from the board's audit committee that includes at least some independent board members and perhaps management.[40] No one form of ERM will fit every firm, and simply designating a CRO or creating a separate risk committee is not enough. All parties involved in the firm's ERM program, including the board, must be engaged in the process.

The question then becomes how to encourage firms to adopt meaningful ERM programs, given the extensive reporting requirements, compliance programs, and operational issues already demanding their upmost attention. Proponents of ERM suggest that comprehensive risk management is not an "add on," but rather an assessment tool that infiltrates all aspects of the business, including reporting and compliance.[41] From this perspective, ERM could streamline existing responsibilities and enhance overall operations and performance results.[42] But this possible upside likely is a tough sale in corporate America, even after the 2008 economic crisis.[43]

ENCOURAGING ERM

Linking ERM to firm profitability likely would accelerate the ERM movement. Most firms seek to maximize returns to investors. Consequently, firms tend to adopt voluntarily (or involuntarily, under market or investor pressure) techniques, like ERM, that potentially enhance those returns.[44] Additional empirical research

---

38. *See, e.g.*, Conference Board Report, *supra* note 9, at 6–7 (recommending six primary tasks for boards considering ERM); Lipton et al., *supra* note 9, at 15–17 (encouraging boards to review committee composition, undertake risk management training, and improve lines of communication).

39. Kirkpatrick, *supra* note 4, at 19 (summarizing findings of a report by the Institute of International Finance (IIF), which examined board performance).

40. *See, e.g.*, Green & Jennings-Mares, *supra* note 35, at 1 (noting that the IIF recommends designating "a Chief Risk Officer (CRO) with sufficient seniority, authority, and independence from line business management to have a meaningful impact on decisions"); Kirkpatrick, *supra* note 4, at 19 (discussing value of CROs and separate risk committees).

41. *See, e.g.*, Conference Board Report, *supra* note 9, at 10 ("ERM should not be seen as an entirely new and separate infrastructure."); COSO Report, *supra* note 8, at 17 (disputing notion that ERM is "something added on to an entity's activities").

42. *See, e.g.*, Conference Board Report, *supra* note 9, at 18 (citing survey data to suggest that, as ERM develops, "directors' perceptions of risk management oversight [will] evolve from a compliance practice to an exercise that is meant to bring clarity, focus and efficiency to the strategy-setting role of the corporate board").

43. *Id.* ("Many directors interviewed resisted what they termed 'an excessively formal' way to incorporate risk management into their deliberations.").

44. *See* Cas. Actuarial Soc'y, Overview of Enterprise Risk Management 27 (2003) (citing examples of organizations implementing ERM and benefiting from increased investment returns and decreased capital

demonstrating the value of ERM—either by increasing profits or reducing losses—is needed and warranted.[45]

Potential legal liability also influences corporate conduct. A board's failure to implement an effective ERM program would appear to breach the board's duty of care. Indeed, without effective ERM, a board arguably is approving overall firm strategy or making other critical decisions without necessary and adequate information.[46] Nevertheless, litigants and courts generally cast ERM claims as failure-to-monitor claims, perhaps because of the barriers to imposing duty of care liability on boards.[47] A failure-to-monitor claim is governed largely by the standards articulated in three Delaware state court decisions,[48] i.e.,

---

requirements); *see also* COSO Report, *supra* note 8, at 1 (noting that ERM enables management to enhance value building capacity).

45. *See* Simkins & Ramirez, *supra* note 9, at 582–83, 585 (citing several studies on ERM and noting that "[o]ne deterrent [to major companies implementing ERM] is the need for more information on implementing ERM, including case studies and educational materials"); *see also* COSO Report, *supra* note 8, at 1 ("Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."). "In addition, ratings agencies, institutional investors, and insurance companies underwriting directors' and officers' liability insurance policies are increasingly focusing on whether companies have ERM processes in place." Conference Board Report, *supra* note 9, at 5.

46. *See, e.g.*, Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1985) (finding the board liable for failing to inform itself of "'all material information reasonably available'" (quoting Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984))). The *Van Gorkom* decision was intensely criticized and subsequently weakened by legislative action. *See* Del. Code Ann. tit. 8, § 102(b)(7) (2009). *See* Bayless Manning, *Reflections and Practical Tips on Life in the Boardroom After* Van Gorkom, 41 Bus. Law. 1 (1985) (criticizing several aspects of *Van Gorkom*). *But see* Lawrence A. Hamermesh, *A Kinder, Gentler Critique of* Van Gorkom *and Its Less Celebrated Legacies*, 96 Nw. U. L. Rev. 595, 595–602 (2002) (acknowledging prior criticisms and considering contributions of case); Lynn A. Stout, *In Praise of Procedure: An Economic and Behavioral Defense of* Smith v. Van Gorkom *and the Business Judgment Rule*, 96 Nw. U. L. Rev. 675, 693 ("The wisdom of the Delaware Supreme Court's decision in Van Gorkom can only be fully appreciated if we are willing to move beyond rational choice, and in particular to recognize the key role that socially contingent altruism may play in shaping the behavior of corporate directors."). Nevertheless, *Van Gorkom* underscores the need for informed board decisions under the business judgment rule. *Van Gorkom*, 488 A.2d at 872.

47. The business judgment rule, exculpation clauses (for example, enacted in accordance with 8 Del. Code Ann. tit. 8, § 102(b)(7)), indemnification agreements, and insurance policies generally protect directors from personal liability for breaches of the duty of care. J. Phil Carlton & M. Guy Brooks, III, *Corporate Director and Officer Indemnification: Alternative Methods for Funding*, 24 Wake Forest L. Rev. 53, 53–55 (1989) (describing the interplay of exculpatory agreements, indemnification agreements, and insurance in protecting directors). The business judgment rule is a presumption that board decisions are made in good faith, on an informed basis and in the best interests of the corporation. *See, e.g.*, *Aronson*, 473 A.2d at 812; *see also In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 52 (Del. 2006); Joan MacLeod Heminway, *Enron's Tangled Web: Complex Relationships; Unanswered Questions*, 71 U. Cin. L. Rev. 1167, 1171–73, 1177–78 (2003) (explaining the power structure of the corporation, the role of the business judgment rule, and the *Van Gorkom* decision as applied in the context of *Enron*). Although certain circumstances involving potential self-interest, conflicts of interest, or undue influence may warrant increased scrutiny of board conduct, ordinary-course board decisions generally garner the protection of the business judgment rule. For a discussion of the business judgment rule in the context of potential conflict situations, see sources and proposal discussed in Michelle M. Harner, *Corporate Control and the Need for Meaningful Board Accountability*, 94 Minn. L. Rev. (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1393883.

48. For an excellent discussion of these three cases and their relation to failure-to-monitor claims, see Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34 J. Corp. L. 967 (2009).

Caremark,[49] *Guttman*,[50] and *Stone*[51]. Under this case trilogy, a failure-to-monitor claim is reviewed in terms of bad faith and duty of loyalty; to succeed, plaintiffs must show "a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists."[52] This standard is difficult to prove, as reiterated by Chancellor Chandler in the *Citigroup* litigation.[53]

In *Citigroup*, the plaintiffs "argue[d] that the director defendants breached their duty of oversight either because the oversight mechanisms were not adequate or because the director defendants did not make a good faith effort to comply with the established oversight procedures."[54] The plaintiffs' primary evidence to support their allegations of misconduct was the board's failure to mitigate Citigroup's risk exposure in response to market and industry indications of problems in the sub-prime market.[55] The plaintiffs did not dispute that Citigroup had risk management controls in place, including a designated audit and risk management committee.[56] Chancellor Chandler characterized the plaintiffs' evidence as, at best, evidence of bad business decisions, which are protected by the business judgment rule.[57] Accordingly, Chancellor Chandler dismissed the plaintiffs' failure-to-monitor claims.[58]

In a thoughtful article, Professor Stephen Bainbridge compares and contrasts ERM with traditional compliance monitoring and analyzes ERM under *Caremark* and its progeny.[59] Professor Bainbridge largely agrees with the result in *Citigroup*, concluding that "[i]f *Caremark* is the most difficult theory of liability in corporate law, risk management needs to be the most difficult variant of *Caremark* claims."[60] He also acknowledges and explains, however, factors in the ERM context that might warrant fiduciary liability.[61]

Professors Betty Simkins and Steven Ramirez present an alternative proposal for encouraging ERM programs through regulatory disclosure requirements.[62] They do not endorse substantive interference in a firm's ERM decisions.[63] Rather, they leave those decisions to the board's discretion and require only disclosure of the firm's

49. *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996).
50. Guttman v. Huang, 823 A.2d 492 (Del. Ch. 2003).
51. Stone v. Ritter, 911 A.2d 362 (Del. 2006).
52. *Caremark*, 698 A.2d at 971.
53. *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 125 (Del. Ch. 2009).
54. *Id.* at 127.
55. *Id.* at 127–28.
56. *Id.* at 127.
57. *Id.* at 128.
58. *Id.* at 139–40.
59. *See* Bainbridge, *supra* note 48, at 975–76, 981.
60. *Id.* at 990.
61. *Id.* at 985–89.
62. *See* Simkins & Ramirez, *supra* note 9.
63. *Id.* at 592.

ERM program and significant risk exposures.[64] The transparency envisioned by the proposal presumably would influence boards to adopt at least some form of ERM.

The growing academic dialogue regarding ERM is welcome and complements nicely the existing business and finance literature. This essay contributes to the dialogue by asking boards, stakeholders, and policymakers to consider the core informational value of ERM.

ERM's informational value

Thinking about ERM solely as a monitoring process undercuts its potential value. An essential component of ERM is a firm-wide monitoring and reporting system. But equally important is the information targeted by the system and transmitted to the board.[65] As discussed above, the board should review, understand, and approve a firm's risk appetite and ongoing risk strategy. A board, in turn, must receive the necessary information and reports to make these decisions.[66] A board's failure to be reasonably informed about risk-related decisions potentially impairs firm performance and ultimate profitability.

Such a failure also may warrant legal liability for the board and senior management. As Chancellor Chandler explained in *Citigroup*: "A plaintiff can show bad faith conduct by, for example, properly alleging particularized facts that show that a director *consciously* disregarded an obligation to be reasonably informed about the business and its risks or *consciously* disregarded the duty to monitor and oversee the business."[67] Bad faith conduct is excluded from the business judgment rule,

64. *Id.* at 593 ("Firms should be required to provide qualitative disclosures regarding their approach to enterprise risk management . . . .").

65. Likewise, an effective ERM program should consider and may improve the communication and sharing of information between the board and shareholders. *See supra* notes 12–14 and accompanying text. In general, "[w]hen a board of directors seeks shareholder action, the fiduciary duty of disclosure, which is a specific application of the duties of care and loyalty, requires that the board 'disclose fully and fairly all material information within the board's control.'" Wayne County Employees Ret. Sys. v. Corti, No. 3534-CC, 2009 Del. Ch. LEXIS 126, at *26 (Del. Ch. July 24, 2009) (quoting Wayne County Employees Ret. Sys. v. Corti, 954 A.2d 319, 330 (Del. Ch. 2008)). Although breaches of the duty of disclosure are often difficult to prove, shareholder communication is an essential component of good corporate governance. Moreover, the board knowingly withholding or failing to disclose information to shareholders may support a finding of bad faith. *See infra* notes 67–71 and accompanying text.

66. *See, e.g.*, OECD Principles of Corporate Governance, *supra* note 19, at 25 ("In order to fulfil [sic] their responsibilities, board members should have access to accurate, relevant and timely information."); *see also* CRMPG Report, *supra* note 37, at 13 ("What [boards] can do, and what management can help them do, is to ask the right questions and insist that they have the information—properly presented—that allows them to exercise their oversight responsibilities.").

67. *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 125 (Del. Ch. 2009); *see also* Stone v. Ritter, 911 A.2d 362, 369 (Del. 2006) (discussing bad faith standard); *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 67 (Del. 2006) (same); Lisa M. Fairfax, *Spare the Rod, Spoil the Director? Revitalizing Directors' Fiduciary Duty Through Legal Liability*, 42 Hous. L. Rev. 393, 417 (2005) (analyzing good faith in the context of the Sarbanes-Oxley Act and noting that courts "have suggested that the fiduciary duty of good faith encompasses a duty to remain informed and to ask appropriate questions of corporate officers"); Hilary A. Sale, *Delaware's Good Faith*, 89 Cornell L. Rev. 456, 494 (2004) ("Fiduciaries who ignore deficiencies in the information they receive or the reporting system on which they rely violate their duty of good faith to the share-

statutory exculpatory clauses, and some indemnification and insurance policies, and it frequently constitutes a breach of the board's duty of loyalty.[68]

A finding of bad faith has teeth, but it also is very difficult to prove. Existing standards require a showing that the board *consciously* disregarded its duty.[69] This standard may nevertheless provide baseline protection in the ERM context.[70] For example, as the ERM discipline matures, firms likely will define more clearly the role of and expectations for the board in ERM. A board's failure to obtain information necessary to satisfy its assigned ERM tasks or make any risk-related decisions may constitute bad faith conduct.[71] If the board receives the information and sim-

---

holders."). The plaintiffs in *Citigroup* did challenge certain board decisions, including approval of a share repurchase program and the CEO's compensation package, but they did so based on allegations of waste and not bad faith or a conscious disregard of the board's duty to be informed. *Citigroup*, 964 A.2d at 111–12.

68. *See, e.g.*, Del. Code Ann. tit. 8 § 102(b)(7) (excluding bad faith conduct from scope of permissible director exculpation provisions); *Stone*, 911 A.2d at 369–70 (explaining that bad faith conduct can be a violation of the duty of loyalty).

69. The term "consciously" generally refers to intentional or knowing conduct. As Chancellor Chandler explained, "A plaintiff can thus plead bad faith by alleging with particularity that a director *knowingly* violated a fiduciary duty or failed to act in violation of a *known* duty to act, demonstrating a *conscious* disregard for her duties." *Citigroup*, 964 A.2d at 125. Some commentators have questioned the Delaware courts' formulation of bad faith and use of the term consciously as potentially subjecting boards to liability for business decisions to, among other things, not consider certain information. *See, e.g.*, Stephen M. Bainbridge, *Good Faith and Risk Taking*, ProfessorBainbridge.com, Oct. 2, 2008, http://www.professorbainbridge.com/professorbainbridge com/2008/10/good-faith-and-risk-taking.html (endorsing an approach similar to that found in the ALI Principles of Corporate Governance and Model Business Corporation Act). For example, section 4.01(c)(2) of the Principles of Corporate Governance requires the board to be "informed with respect to the subject of the business judgment to the extent the director or officer reasonably believes to be appropriate under the circumstances." ALI Principles of Corporate Governance, *supra* note 20, at § 4.01(c)(2). *But see* Sale, *supra* note 67, at 495 (reviewing the courts' articulation of good faith and concluding that "[s]uch strong enforcement of good faith standards by the stewards of state corporate law contributes to good corporate governance norms"). Courts should strive to preserve board discretion to operate the business. *See, e.g.*, Stout, *supra* note 46, at 693 (commending the Delaware Supreme Court's decision in *Van Gorkom* for having the "wisdom to concede that it was unqualified to sit in judgment on the substantive wisdom of most corporate directors' business decisions"). Nevertheless, insulating every board decision, such as what information to seek and review, from judicial review guts even the gross negligence and bad faith standards articulated by courts to balance authority and accountability in the corporate governance context. *See, e.g.*, Fairfax, *supra* note 67, at 411(noting that the business judgment rule was a "'nearly insurmountable' barrier to director liability, with *Van Gorkom* standing out as the 'one major instance in which nonconflicted managers were held liable to pay for their mismanagement'" due to their failure to seek information necessary to inform their decision (citation omitted)). Courts can determine whether a firm's ERM program provided the board with sufficient information regarding the decision at hand without reviewing the merits of the underlying substantive board decision. *See, e.g.*, Stout, *supra* note 46, at 693 (commenting that the *Van Gorkom* court "focused on what it could judge—the quality and thoroughness of the directors' business decision-making process"). Moreover, the business judgment rule places the initial burden on the plaintiff to show that the decision was uninformed. *See Citigroup,* 964 A.2d at 125 ("[T]he burden required for a plaintiff to rebut the presumption of the business judgment rule by showing gross negligence is a difficult one, and the burden to show bad faith is even higher.").

70. Neither ERM nor this essay aims to penalize boards; rather, the goal is informed board and firm action on risk-related decisions. Accordingly, the higher standard of bad faith may be an appropriate balance between protecting boards that try to do it right (but get the ultimate decision wrong) and those that do not even try.

71. Notably, boards and board committees frequently are called upon to make decisions that may not directly relate to the ERM program but involve risk assessment and response. *See* Lipton et al., *supra* note 9, at 15 (emphasizing need for the entire board to receive risk information because "risk management issues may arise in the context of the work of other committees, and the decision-making in those committees should take

ply makes a bad decision, its conduct is within the existing protections of the business judgment rule.[72]

Reflecting on the 2008 economic crisis, the key question then becomes what boards knew and whether that information was adequate to decide the issues before them. A potential critique of this approach is that boards simply could elect to implement ERM programs that delegate all risk decisions to management and a designated CRO. In fact, that likely is the case for many firms that experienced losses during the crisis.[73] As discussed above, such a silo approach to ERM is counter-productive for firms. Consequently, market forces and regulatory reforms can encourage appropriate allocation of ERM responsibilities, strengthened by the board's duty to be reasonably informed in executing its ERM role.

extracting erm's informational value

A primary goal of ERM, like most corporate governance initiatives, is to better equip boards and management to operate productive and ethical firms.[74] Encouraging boards to be involved and informed in ERM decisions furthers this goal. Regulatory, legislative, and judicial responses to the ERM movement should likewise pursue this objective.

A board should be involved with a firm's ERM program from its inception. To this end, a board may need risk-assessment training and additional, ongoing education regarding the firm's various business divisions, opportunities, and risks.[75] This additional knowledge not only will assist the board in evaluating ERM programs and setting the firm's overall risk appetite, but also will enable the board to ask more informed questions of management and professionals and make more informed decisions generally.

The board's specific tasks in any ERM program may vary based on the firm or industry, as the ERM program should be tailored to the needs of the particular firm. Nevertheless, in most firms, the board should evaluate and approve the ERM program; establish the firm's overall risk appetite; ensure that appropriate day-to-

---

into account the company's overall risk management system"). For example, the Emergency Economic Stabilization Act of 2008 requires that participants include "limits on compensation that exclude incentives for senior executive officers of a financial institution to take unnecessary and excessive risks that threaten the value of the financial institution." Emergency Economic Stabilization Act of 2008, Pub. L. No. 110-343, §111(b)(2)(A), 122 Stat. 3765, 3776–77.

72. *See* Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984) (discussing the court's obligation to respect business decisions under the business judgment rule if the presumptions that the corporation "acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company" are not overcome).

73. Kirkpatrick, *supra* note 4, at 1, 11–12 (discussing the impact of failure and weaknesses in ERM on susceptibility to excessive risk taking during the financial crisis).

74. COSO Report, *supra* note 8, at 1, 3 (discussing ERM's role in enhancing management's capacity to build value and in setting the basis for integrity and ethical values in assessing risk).

75. *See* Conference Board Report, *supra* note 9, at 7–8 (recommendations for boards regarding ERM, including risk assessment training); Lipton et al., *supra* note 9, at 14–17 (same).

day monitoring and reporting procedures are in place across the firm; and schedule regular board (or board committee) meetings dedicated to reviewing and reassessing the firm's risk exposure and response measures.[76] In performing these tasks, the board should strive to create an ERM program that links risks at all levels of the firm and incorporates risk assessment into every major board and management decision.

These observations regarding the board's role in ERM are based, in part, on the board's traditional oversight role in corporate governance. They also reflect the board's duty to act in good faith and on an informed basis. Accordingly, these observations may serve as useful guidelines as boards work with managers and consultants to design effective ERM programs and as stakeholders and policymakers consider the value of ERM.

CONCLUSION

ERM promotes a "big picture" approach to risk management.[77] It recognizes that various events may converge to increase a firm's risk exposure and resulting losses.[78] An effective risk management structure accounts for potential risks in all aspects of a firm's operation and analyzes the firm's overall risk appetite and response strategy.[79] The 2008 economic crisis is the poster child for improving risk management practices and, hopefully, will motivate boards, stakeholders, and policymakers to promote meaningful ERM programs.

76. *See supra* notes 35–43 and accompanying text. Some commentators suggest that risk reports from all business divisions flow to a single department or committee that has direct access to the board and senior management. *See supra* note 28 and accompanying text. That department or committee also may include members of the board or senior management. Boards need ERM structures that provide real-time risk reports to make informed risk and other decisions.

77. COSO Report, *supra* note 8, at 1 ("Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.").

78. *Id.*

79. *Id.* ("Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.").