Director Notes

The Potential Cost and Value of ERM

by Michelle Harner

The concept of enterprise risk management (ERM) as a holistic approach to managing a company's risk profile has tremendous appeal. However, companies are frequently skeptical about its value and whether the results will justify the cost, effort, and challenges of implementing a meaningful ERM process.[1] This report considers some of those concerns and highlights the governance, compliance, and cultural value of ERM.

Risk management is not a new concept. Companies have been, at the very least, considering and modeling financial risk for quite some time.[2] ERM is a holistic approach to managing a company's risk profile.[3] It encourages boards of directors to foster and embrace a risk-aware culture that supports firm-wide communication. By empowering individuals at multiple levels within and across an organization to identify, assess, and communicate about risk exposure, boards can more effectively work with their management teams to mitigate and monitor risks.[4] The objective of ERM is not to eliminate all risks, but rather to maintain a level of risk that aligns with the company's risk appetite.[5]

Despite ERM's potential benefits, conversations about implementing it are often informal, disjointed, siloed, and incomplete.[6] Moreover, the failings of a company's risk management approach typically are not exposed until times of crisis or distress. The corporate scandals of 2001–02 and the economic recession of 2007–2008 offer numerous examples of risk management breakdowns and hindsight or reactive responses to those failings.[7]

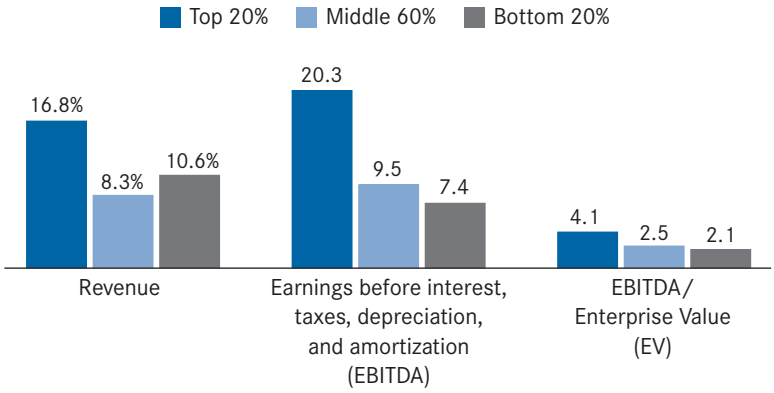
No. DN-V5N5
MARCH 2013

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

Chart 1

Compound annual growth rates 2004–11* by risk maturity level

Companies with more mature risk management practices generated the highest growth in revenue, EBITDA, and EBITDA/EV.



* 2011 YTD reported as of November 18, 2011.

Source: Ernst & Young, *Turning Risk into Results: How Leading Companies Use Risk Management to Fuel Better Performance*, February 2012.

An Overview of ERM Concepts

In business, tension often exists between risk management and profit maximization. Boards and managers must constantly strive to strike an appropriate balance between the two. The corporate scandals and general failures of the early 2000s highlighted the difficulties in managing this tension. In response, the government developed new risk-related disclosure regulations and a new framework for risk management.[8] These included the Sarbanes-Oxley Act, new listing standards for the New York Stock Exchange (NYSE), and the U.S. Department of Justice's revised sentencing guidelines.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed an ERM framework to assist companies with operating in this new regulatory environment. ERM is "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."[9] ERM focuses on the potential risks to and related consequences for the entire company—not just the specific departments or units responsible for foreseeable risks or risk-seeking activities.[10]

Commentators frequently quote the proverb "no risk, no reward" in the business context. Yet, calculated risk is fundamentally different from rash or unmitigated risk. The latter often leads to negative consequences, including significant economic losses, litigation, missed business opportunities, and failed business models. Boards must strive to proactively identify and evaluate their companies' risk profiles and accept only calculated risks that are commensurate with their companies' risk appetites. ERM is a key tool in this endeavor.

At its core, ERM encourages companies to develop a disciplined process for identifying, assessing, mitigating, and monitoring potential risks to the enterprise through both vertical and horizontal prisms. This approach requires a company to look within its individual entities, departments, and units, and then across those divisions to create a more complete risk picture. In this regard, COSO's model for implementing ERM seeks to identify risks to the company's objectives at every level of the enterprise (e.g., entity, department, unit) while focusing assessment and mitigation plans on eight interrelated components:[11]

1 Internal environment

2 Objective setting

3 Event identification

4 Risk assessment

5 Risk response

6 Control activities

7 Information and communication

8 Monitoring

COSO suggests that effective implementation of ERM requires a top-down approach, with the board playing a critical role in fostering a risk-aware culture, setting the company's risk appetite, and reconciling that appetite with the company's risk profile.[12]

Procedures for implementing effective ERM programs are still emerging.[13] ERM implementation requires the board and senior management to map out the company's business strategies and potential barriers to those strategies. In fact, many companies use their strategic plans as blueprints for their ERM programs. A successful ERM program capitalizes on the synergies between mitigating a company's risk exposure and achieving its strategic and operational objectives.[14]

Boards must understand all elements of potential risks to align them with their companies' risk appetites and strategic plans. That level of understanding requires effective communication across the enterprise, which companies can foster by establishing clear channels of communication and identifying risk owners. Many companies have implemented reporting systems for allegations concerning harassment, discrimination, and illegal activity. In fact, these types of whistleblower provisions are often incorporated into companies' codes of ethics.[15] Developing similar reporting systems for the identification of potential operational or financial risk events is one path to encourage meaningful risk communication.[16]

There is no one right way to implement ERM, and companies should tailor their ERM programs to their particular industry, strategic plan, and internal needs. Focusing on communication channels and risk ownership will help companies integrate risk assessment throughout the enterprise. Integration, in turn, will reduce the likelihood that risks become trapped in silos and underappreciated by boards and senior management.[17]

Corporate Governance Considerations

In the United States, state law typically vests the board with management authority over the corporation.[18] Directors serve in a fiduciary capacity, with the company and its shareholders as the primary beneficiaries.[19] As such, directors owe duties of care and loyalty, with the latter generally including an obligation of good faith.[20] The duty of care generally requires directors to be fully informed and diligent when making their business decisions.[21] The duty of loyalty mandates, among other things, that directors remain free from conflicts and act selflessly, in good faith, and with the corporation's best interests at heart.[22]

An effective ERM program may help directors comply with their fiduciary duties in multiple respects. For example, in evaluating duty of care claims, courts typically consider whether directors were informed regarding the issue under consideration, made reasonable inquiries concerning the matter, understood key components and critiques of the proposed action, and were deliberative in their decision-making process.[23] ERM contributes positively to several of these factors.[24] The enhanced communication and information flow underlying ERM should strengthen the utility of boards' decision-making processes, making it more difficult for plaintiffs to overcome the board's traditional protection under the business judgment rule.[25]

Moreover, monitoring and managing a company's risks are at the core of ERM, which directly implicates directors' duty to monitor. "The duty to monitor is an obligation to prevent harm to the corporation."[26] Although originally perceived as a subset of the duty of care, duty to monitor claims are now commonly viewed as invoking standards applicable to duty of loyalty claims. These standards require that plaintiffs establish, at a minimum, a knowing dereliction of duty or "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."[27] As the Delaware Court of Chancery explained in *In re Citigroup Inc. Shareholder Derivative Litigation*, these standards create an "extremely high burden" for plaintiffs.[28]

In *Citigroup*, the plaintiffs argued that the directors breached their duty to monitor by not mitigating Citigroup's risk exposure. Citigroup's substantial investment in mortgage-backed securities was a risk that led to significant shareholder losses and government bailouts. The plaintiffs argued that the Citigroup board ignored indicators of the deteriorating subprime mortgage market. Although the court recognized a board's heightened duty to act when "red flags" suggest wrongdoing at the company, it found that the plaintiffs' evidence was, at best, evidence of bad business decisions.[29] The court rejected the plaintiffs' asserted duty to monitor claims and granted the defendants' motion to dismiss.

The business judgment rule ultimately protected the board's decisions in *Citigroup* and in similar cases involving AIG and Goldman Sachs.[30] Nevertheless, individuals serving on those boards were named as defendants in very high-profile, expensive lawsuits, and their decisions apparently did cause economic harm to their companies and shareholders—so any victory they attained was bittersweet in some respects. In addition, *Citigroup* and subsequent cases leave open the possibility of director liability for failures in monitoring and oversight.[31] As then-Chancellor William 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."[32]

A thoughtful and integrated ERM program may enhance board protections in litigation and, more importantly, improve its decision-making processes. A board that implements and nurtures an ERM program will be overseeing the active identification and management of potential risks to the enterprise. If structured appropriately, the program should foster more complete and meaningful risk reports to the board and more coordinated responses to both enterprise-level risks and those being managed by individual departments and units. Indeed, an effective ERM program might well serve as a prophylactic measure against any purported breaches of the duty to monitor.

Regulatory Compliance Considerations

The corporate scandals of the early 2000s and the economic crisis of 2008 have led to enhanced regulation of company activities on multiple fronts. For example, Sarbanes-Oxley enhanced standards for corporate governance and reporting. The SEC amended its proxy guidelines to require disclosure of the board's role in the company's risk management.[33] The NYSE likewise revised its listing standards to redefine corporate independence, addressing both internal controls and codes of ethics, and specifically identifying risk management as a function of an audit committee.[34] Companies that fail to comply may be subject to agency investigations, litigation, and sanctions.[35]

Regulatory compliance is an integral part of ERM. A company cannot assess accurately its risk profile without a comprehensive understanding of the regulatory environment in which it operates. ERM may itself help a company comply with applicable regulations, reduce the impact of certain compliance failures, and produce other external benefits. For example, Standard & Poor's considers the existence of an ERM program in rating any given company.[36] ERM can complement and strengthen a company's existing internal controls, code of ethics, and compliance culture.

Other Considerations

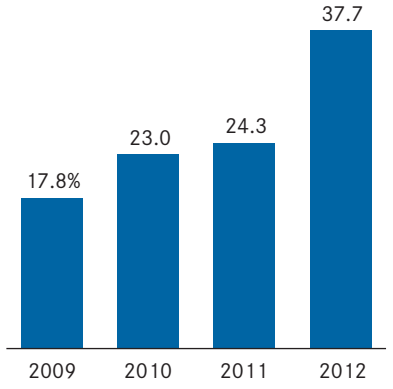
In light of the potential governance and compliance benefits, the question shifts from why a company should implement ERM to why it would not. Like most initiatives, ERM has potential costs and implementation challenges that may limit its positive impact.[37] The following section summarizes certain countervailing factors. Although each company must make its own assessment, on balance, ERM appears well worth the effort.

Increased cost ERM may be viewed as yet another layer of administrative expense that increases overhead and negatively impacts the bottom line.[38] That perception may hold some truth. Companies may hire a chief risk officer or need additional personnel and resources to implement an ERM program. Some companies retain outside consultants to design their ERM programs and address related programmatic needs. ERM may also identify risks or potential issues that require mitigation plans and the expenditure of considerable resources to support those plans. Companies should be aware of the potential costs associated with any ERM program and factor those into their cost-benefit analysis.

Chart 2

Designated individual to serve as CRO or equivalent

There has been a notable increase over prior years in the percentage of organizations that have formally designated an individual to serve as the chief risk officer (CRO) or equivalent senior risk executive.



Source: Mark Beasley, Bruce Branson, and Bonnie Hancock, "Current State of Enterprise Risk Oversight: Progress Is Occurring but Opportunities for Improvement Remain," July 2012, 17.

Additional work Similarly, ERM may be viewed as creating additional "busy work" that distracts managers from their primary responsibility—running the business.[39] This view of ERM as a "check-the-box" exercise done outside of ordinary job responsibilities undercuts the true value of ERM. Employees at all levels should identify and assess potential risks in the ordinary course of business on a daily basis. ERM is designed, in part, to underscore the importance of this integrated risk assessment—a task that boards, managers, and employees already should be undertaking. ERM is not new or additional work; it is a more disciplined and effective way to perform that work.

Impede innovation A pure risk identification and mitigation approach to ERM might suggest that companies forgo valuable, yet risky, opportunities. In other words, ERM might cause companies to become too risk averse.[40] That should not be the objective or result of a properly structured ERM program. Rather, companies should use ERM to reduce barriers to innovation and foster projects within the companies' risk appetites.[41]

Minimal impact ERM has received mixed reviews regarding its impact on the bottom line. Some companies appear to have gotten lost in the process—almost paralyzed by the information output. A company that becomes consumed by the process itself or is unable to discern and address entity level and emerging risks likely will not realize much value from an ERM process.[42] As one commentator notes, "ERM is only as effective as it is able to produce a risk radar that is meaningful and forward looking."[43] The value in ERM comes from understanding the companies' objectives and designing an ERM program that minimizes barriers to the company's forward trajectory.

Misunderstood Boards may reject ERM because they do not understand the concept or its application to their company. In 2011, a study of corporate directors indicated that boards have not increased the amount of time spent on reviewing and approving company risk management strategies and that they lack the requisite knowledge to do so.[44] Directors reported dedicating only 14 percent of their time to risk management.[45] In addition, boards may assign primary responsibility for ERM functions to the accounting or financial departments and, in the process, lose sight of the cross-functional goal of ERM.[46] Accordingly, before adopting any ERM program, boards should take the time to understand ERM and how it might assist the company in achieving its objectives.

Potential Upside with Little Downside Risk

ERM can facilitate sound corporate governance practices that are likely to have a positive impact on multiple aspects of a company's operations.[47]

With proper planning, companies can implement ERM in a manner that mitigates more than financial risk. They can improve communication and discipline in their decision-making processes and address cross-functional risks such as legal, operational, and personnel matters. In addition, effective ERM programs may help boards comply with various legal rules and regulations and satisfy their fiduciary duties to companies and shareholders.

Admittedly, there are challenges associated with ERM, and companies should not undertake an ERM program half-heartedly. Nonetheless, studies suggest that, if executed properly, ERM increases the flow of risk information and leads to better-informed decisions, greater consensus, and better communication with management—i.e., better management.[48] "Better management translates into the increased ability to meet strategic goals, reduced earnings volatility, and increased profitability."[49] Accordingly, any downside risk associated with ERM likely is outweighed by its potential value.

Table 1

Companies with advanced ERM experience greater returns.

	Advanced ERM companies		All other companies	
	Rank	Percent	Rank	Percent
Better informed decisions**	1	86%	1	58%
Greater management consensus***	2	83	2	36
Increased management accountability***	3	79	3	34
Smoother government practices***	4	79	4	39
Ability to meet strategic goals***	5	76	5	36
Better communication to board+	6	69	6	52
Reduced earnings volatility**	7	62	7	37
Increased profitability**	8	59	8	33
Use risk as competitive tool**	9	46	9	22
Accurate risk-adjusted pricing*	10	41	10	21

*** 99.9% likelihood of significant difference between advanced ERM and all other companies

** 99% likelihood of significant difference between advanced ERM and all other companies

* 95% likelihood of significant difference between advanced ERM and all other companies

+ 90% likelihood of significant difference between advanced ERM and all other companies

Source: Matteo Tonello, *Emerging Governance Practices in Enterprise Risk Management*, The Conference Board R-1398-07-WG, February 2007.

Endnotes

1 Mark Beasley, et al., "Current State of Enterprise Risk Oversight: Progress is Occurring But Opportunities for Improvement Remain," July 2012, p. 32 (http://poole.ncsu.edu/vol2/erm/ee/i/weblogs/research-documents/AICPA_ERM_Research_Study_2012_Final_Submission_July_16,_2012.pdf). Although there is limited empirical evidence supporting the implementation of ERM, studies indicate that companies with advanced ERM experience, among other things, reduced earnings volatility and increased profitability. See Matteo Tonello, *Emerging Governance Practices in Enterprise Risk Management*, The Conference Board R-1398-07-WG, February 2007.

2 Tonello, *Emerging Governance Practices in Enterprise Risk Management*. Risk management first appeared as an enterprise-wide structure in the late 1980s. The debate continued in the 90s, particularly after the Enron scandal.

3 Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management-Integrated Framework: Executive Summary," September 2004, p. 2 (www.coso.org/documents/coso_erm_executivesummary.pdf) [COSO Report].

4 Michelle M. Harner, "Ignoring the Writing on the Wall: The Role of Enterprise Risk Management in the Economic Crisis," *Journal of Business & Technology Law*, 2010, pp. 45, 48.

5 "An organization's risk appetite, or willingness to take risk, reflects both its capacity to bear risk as well as a broader understanding of the level of risk that it can safely and successfully manage for an extended period. Risk appetite represents the executive management's 'view of the world' that drives strategic choices, and is expressed over time through an entity's actions or inactions." Protiviti, *Performance/Risk Integration Management Model – PRIM²: Early Mover Series – Analyzing Strategic Risk,* 2011, p. 6, (www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/PRIM2-Early-Mover-Analyzing-Strategic-Risk-Protiviti.pdf).

6 See generally, Beasley, et al., "Current State of Enterprise Risk Oversight," discussing survey data indicating many companies have no formal risk management process in place and many others have immature programs.

7 In 2007, the world's largest banks began feeling the impact of the U.S. subprime mortgage crisis. In 2008, Bear Stearns faced failure and the FDIC took over Indymac Bank. The term "financial crisis" was also coined in 2008 as the financial system took a downward spiral. The government took over Fannie Mae and Freddie Mac. Merrill Lynch was forced to sell, Lehman Brothers failed, and the federal government rescued AIG. See Tonello, *Emerging Governance Practices in Enterprise Risk Management*. See also David M. Kotz, "The Financial and Economic Crisis of 2008: A Systemic Crisis of Neoliberal Capitalism," *Review of Radical Political Economics* 41, no. 3, 2009, p. 305 (http://rrp.sagepub.com/content/41/3/305.full.pdf+html); Robert Prentice, "Enron: A Brief Behavioral Autopsy," *American Business Law Journal* 40, no. 2, December 2002, p. 417, discussing the business practices leading to the Enron scandal and the congressional actions that followed; Robert Eli Rosen, "Risk Management and Corporate Governance: The Case of Enron," *Connecticut Law Review* 35, no. 1157, 2003, discussing the corporate governance problems of Enron as a redesigned corporation and its risk-management practices; and J. Gregory Sidak, "The Failure of Good Intentions: The WorldCom Fraud and the Collapse of American Telecommunications After Deregulation," *Yale Journal on Regulation,* 2003, p. 207, discussing Worldcom's fraud and bankruptcy and the implications on the telecommunications industry.

8 See, e.g., Troy A. Paredes, "Foreword to After the Sarbanes-Oxley Act: The Future of the Mandatory Disclosure System," *Washington University Law Quarterly* 81, no. 2, 2003, p. 229, explaining the events leading up to the corporate scandals of the early 2000s and the regulatory and legislative responses.

9 COSO Report, p. 2.

10 See, e.g., Dr. Larry Rittenberg and Frank Martens, "COSO Enterprise Risk Management: Understanding and Communicating Risk Appetite," 2012, p. 1, (www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf) ("ERM is not isolated from strategy, planning, or day-to-day decision making. Nor is it about compliance. ERM is part of an organization's culture…").

11 COSO Report, p. 2.

12 Rittenberg and Martens, "COSO Enterprise Risk Management: Understanding and Communicating Risk Appetite," p. 1.

13 Stephen Gates, et al., "Enterprise Risk Management: A Process for Enhanced Management and Improved Performance," *Management Accounting Quarterly* 13, no. 3, Spring 2012, p. 29.

14 Michelle M. Harner, "Barriers to Effective Risk Management," *Seton Hall Law Review* 40, no. 4, 2010, pp. 1323, 1334.

15 See generally Richard Moberly and Lindsey E. Wylie, "An Empirical Study of Whistleblower Policies in the United States Corporate Codes of Ethics," in *Whistleblowing and Democratic Values,* eds. David Lewis and Wim Vandekerckhove, (International Whistleblowing Research Network, 2011) describing the history and scope of whistleblower provisions and their use in corporate codes of ethics.

16 For example, some companies implement coordinated risk assessment processes at the board, department, and unit levels. This segmented approach allows the board to focus on strategic and global risks while encouraging others within the organization to manage the more day-to-day operational risks. Appropriate reporting and communication channels link these efforts under an integrated ERM program. See Carol A. Fox and Michael S. Epstein, "Why Is Enterprise Risk Management (ERM) Important for Preparedness?" (www.disaster-resource.com/articles/08p_022.shtml) last visited Jan. 2, 2013, explaining one such approach to enhance disaster preparedness plans.

17 At least one study suggests that financial institutions with more integrated risk-management programs performed better during the 2008 recession. See Harner, "Barriers to Effective Risk Management," p. 1335. See also Senior Supervisors Group, "Observations on Risk Management Practices During the Recent Market Turbulence," 2008, (www.newyorkfed.org/newsevents/news/banking/2008/SSG_Risk_Mgt_doc_final.pdf).

18 See Del. Code Ann. tit. 8, § 141(a) (2001) ("The business and affairs of every corporation...shall be managed by or under the direction of a board of directors ...."); Model Bus. Corp. Act Ann. § 8.01(b) (4th ed. 2008) ("All corporate powers shall be exercised by or under the authority of the board of directors of the corporation, and the business and affairs of the corporation shall be managed by or under the direction, and subject to the oversight, of its board of directors ...."); N.Y. Bus. Corp. Law § 701 (McKinney) ("[T]he business of a corporation shall be managed under the direction of its board of directors.").

19 *N. Am. Catholic Educ. Programming Found., Inc. v. Gheewall*a, 930 A.2d 92 (Del. 2007); *Dodge v. Ford Motor Co.*, 204 Mich. 459, 507, 170 N.W. 668, 684 (1919); *Model Bus. Corp. Act Ann.* § 8.01(b) (4th ed. 2008). Directors also may owe duties to the company's creditors in certain circumstances depending on the company's financial condition. See, e.g., Gheewalla, 930 A.2d, pp. 101-103.

20 20 See, e.g., *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 369-70 (Del. 2006); Model Bus. Corp. Act. Ann. § 8.30 (4th ed. 2008). See also *In re* Walt Disney Co. Derivative Litig., 907 A.2d 693 (Del Ch. 2005) *aff'd*, 906 A.2d 27 (Del. 2006).

21 See, e.g., *Smith v. Van Gorkom*, 488 A.2d 858, 872 (Del. 1985) (explaining that, under Delaware law, "prior to making a business decision, [directors must be informed] of all material information reasonably available to them"). See also *Stone*, 911 A.2d at 368.

22 Stone, 911 A.2d at 370 (quoting *Guttman v. Huang*, 823 A.2d 495, 506 n.34 (Del. Ch. 2003)).

23 See, e.g., William M. Lafferty, et al., "A Brief Introduction to the Fiduciary Duties of Directors Under Delaware Law," *Penn State Law Review* 116, 2012, pp. 837, 842-43, explaining factors relevant to court's decisions in actions alleging breaches of directors' duty of care.

24 A survey of organizations ranging in size and fields, including finance and energy, indicated a direct positive correlation between ERM and internal communication. Carol Fox, "The ERM Tipping Point," *Risk Management Magazine,* Nov. 1, 2011, (http://rmmagazine.com/2011/11/01/the-erm-tipping-point/).

25 The business judgment rule is a presumption that directors act in good faith, on an informed basis and in the best interests of the company when making business decisions. The presumption places the initial burden on the plaintiff in any litigation alleging breaches of the duty of care. Plaintiffs generally must show fraud, illegality, or a breach of the duty of loyalty to overcome the protections of the business judgment rule. If a plaintiff makes a sufficient showing, the burden in the litigation typically shifts to the defendants to show that the transaction or decision in dispute was entirely fair to the company. There are variations on these standards depending on the nature of the allegations and the governing law. See, e.g., *Aronson v. Lewis*, 473 A.2d 805, 812 (Del. 1984) (noting, in the context of demand futility, a presumption that directors making business decisions act on an informed basis, in good faith, and in the honest belief the action was taken in good faith; the party challenging the decision carries the burden of rebutting the presumption); *Van Gorkom*, 488 A.2d at 874 (noting the presumption of the business judgment rule can be rebutted by showing the board was not adequately informed, for example); *Bayer v. Beran*, 49 N.Y.S.2d 2, 8-9 (1944) describing how the burden will shift back to directors, even if there is a potential breach of loyalty, who can avoid liability by proving the transaction was intrinsically fair to the corporation.

26 Eric J. Pan, "A Board's Duty to Monitor," *New York Law School Law Review* 54, 2009, pp. 717, 720.

27 *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996). The Delaware Supreme Court restated and explained these standards in *Stone*, 911 A.2d at 368-70. See also Pan, "A Board's Duty to Monitor," pp. 720-21.

28 *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 125 (Del. Ch. 2009).

29 *In re* Citigroup Inc. S'holder Derivative Litig at 128.

30 *In re* Goldman Sachs Group, Inc. S'holder Litig., Civ. No. 5215-VCG, 2011 WL 4826104 at *22 (Del. Ch. Oct. 12, 2011) ("the essence of their complaint is that [the court] should hold the Director Defendants 'personally liable for making (or allowing to be made) business decisions that, in hindsight, turned out poorly for the Company.' If an actionable duty to monitor business risks exists, it cannot encompass any substantive evaluation by a court of a board's determination of the appropriate amount of risk. Such decisions plainly involve business judgment."); *In re* Am. Int'l Group, Inc. Derivative Litig., 700 F. Supp. 2d 419, 436 (S.D.N.Y. 2010) *aff'd*, 415 F. App'x 285 (2d Cir. 2011) (Plaintiffs alleged violation of federal securities laws and for breaches of fiduciary duty, waste of corporate assets, unjust enrichment, and contribution—all based on management's alleged failure to properly oversee the company's credit default swap contracts, which significantly involved subprime mortgage-backed financial products, material misstatements regarding the company's financial health and risk management, the board's decision to increase the company's dividend payment, the authorization and execution of a stock repurchase plan shortly before the company faced a liquidity crisis, and approval of certain compensation arrangements with certain executives and personnel. The court determined the plaintiff had failed to plead sufficient facts demonstrating liability under Caremark standards.).

31 See, e.g., *Am. Int'l Group v. Greenberg,* 965 A.2d 763 (Del. Ch. 2009) (denying motion to dismiss, among other things, plaintiffs duty to monitor claims; notably, the court in *Citigroup*, 964 A.2d at 130, distinguished this case as one alleging a failure to monitor legal or compliance risks as opposed to business risks); *In re* Am. Int'l Group, Inc. ERISA Litig. II, No. 08 Civ. 5722, 2011 WL 1226459 (S.D.N.Y. Mar. 31, 2011) (denying motion to dismiss, among other things, allegations concerning failure to monitor certain fiduciaries); La. Mun. Police Emples. Ret. Sys. v. Pyott, 46 A.3d 313 (Del. Ch. 2012) (denying motion to dismiss, among other things, duty to monitor claims). See also *Goldman Sachs,* 2011 WL 4826104, at *22 ("[I]mposing *Caremark-type* duties on directors to monitor business risk is fundamentally different from imposing on directors a duty to monitor fraud and illegal activity.").

32 *Citigroup*, 964 A.2d at 125. See also *Stone*, 911 A.2d at 367; *In re* Walt Disney Co. Derivative Litig., 907 A.2d 693, 755 (Del. Ch. 2005) (internal quotation omitted).

33 Proxy Disclosure Enhancements, Exchange Act Release No. 33-9089, 17 C.F.R. §§ 229, 29, 240, 249, 274 (Dec. 16, 2009), corrected by Exchange Act Release No. 33-9089A, 17 C.F.R. § 249 (Feb. 3, 2010). Risk must be reported to the extent it arises from a company's compensation policies and practices and are reasonably likely to have a material adverse effect on the company.

34 Harner, "Barriers to Effective Risk Management," p. 1331. In addition, at least one proposal urged mandatory risk monitoring. See Shareholder Bill of Rights Act, S. 1074, 111th Cong. (2009). Although not enacted, this bill was introduced on May 19, 2009, and sponsored by Senator Charles E. Schumer (D-NY).

35 Notably, after investigating the cause of the financial crisis, the Financial Crisis Inquiry Committee suggested that the financial crisis was avoidable and attributed some responsibility to failures in corporate governance, including failure to properly manage risk. U.S. Financial Crisis Inquiry Commission, "The Financial Crisis Inquiry Report on the Causes of the Financial and Economic Crisis in the U.S.," 2011, p. xviii , (http://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_full.pdf). Such attention to risk failures likely has increased scrutiny and raised expectations.

36 Michael K. McShane, et al., "Does Enterprise Risk Management Increase Firm Value?" *Journal of Accounting, Auditing & Finance* 26, no. 4, 2011, p. 641. Fitch Ratings, Moody's, and A.M. Best Company also have considered models that take ERM into account. See Grant Thornton LLP, "Enterprise Risk Management: Creating Value in a Volatile Economy," CorporateGovernor Series, Summer 2009, p. 6 (www.gt.com/staticfiles/GTCom/Advisory/CorporateGovernor/CGwhitepaper_ERM_FINAL.pdf).

37 Tim J. Leech, "Risk Oversight, The High Cost of 'ERM Herd Mentality,'" March 2012, (http://riskoversight.ca/wp-content/uploads/2011/03/Risk_Oversight-The_High_Cost_of_ERM_Herd_Mentality_March_2012_Final.pdf); Michael Power, "The Risk Management of Nothing,"*Accounting, Organizations & Society*, Vol. 34, 2009, pp.849, 853-54, positing that ERM is a symptom of past shortcomings rather than a "cure for the future" because ERM frameworks overemphasize financial and accounting measures as a mechanism for measuring risk; Dermot Williamson, "The COSO ERM Framework: A Critique from Systems Theory of Management Control," *International Journal of Risk Assessment and Management* 7, no. 8, 2007, p. 1089, arguing the COSO framework has serious limitations, including failure to provide a workable standard for determining ERM effectiveness.

38 Rittenberg and Martens, "COSO Enterprise Risk Management: Understanding and Communicating Risk Appetite," p. 2, noting that management may argue that "risk is considered when management sets strategies, and to further communicate risk appetite is an exercise that simply adds overhead and does not contribute to organizational growth." See also Leech, "Risk Oversight, The High Cost of '"ERM Herd Mentality,'" pp. 3-4, discussing the high costs of implementing an ERM program and complying with Sarbanes-Oxley § 404.

39 See, e.g. Donald C. Langevoort, "The Social Construction of Sarbanes-Oxley," *Michigan Law Review* 105, no. 8, June 2007, pp. 1817, 1831, 1836, noting that board members may be overly distracted by Sarbanes-Oxley reforms and ERM; Brian W. Nocco and René M. Stulz, "Enterprise Risk Management: Theory and Practice," *Journal of Applied Corporate Finance* 18, no. 4, Fall 2006, pp. 8,15, noting that internal business units may resist ERM monitoring and oversight because such efforts "are time-consuming and distract from other activities."

40 Martin Lipton, et al., "Risk Management and the Board of Directors," *Bank and Corporate Governance Law Reporter* 45, no. 6, February 2011, pp. 793, 784, "Running a company is an exercise in managing risk in exchange for potential returns, and there can be danger in excessive risk aversion, just as there is danger in excessive risk-taking."

41 See Protiviti, "Performance/Risk Integration Management Model," p. 9, discussing how defining strategic assumptions helps drive innovation. See also Michael Alix, "Risk Governance: Appetite, Culture and the Limits of Limits," Remarks at the Risk USA 2012 Conference, November 14, 2012, (www.newyorkfed.org/newsevents/speeches/2012/alix121114.html).

42 Tim Leech, "Board Oversight of Management's Risk Appetite and Tolerance," The Conference Board, *Director Notes*, December 2012, pp. 1-2, noting that companies that use a traditional, more static approach, to ERM have been disappointed with the results, (www.conference-board.org/retrievefile.cfm?filename=TCB-DN-V4N23-12.pdf&type=subsite).

43 PricewaterhouseCoopers, "Extending Enterprise Risk Management (ERM) to Address Emerging Risks," 2009, p. 3. Wal-Mart's experience often is cited as a successful implementation of an ERM strategy. See William Atkinson, "Risk Management at Wal-Mart," *Risk Management Magazine,* December 2003, pp. 36, 38.

44 McKinsey & Co, "Governance Since the Economic Crisis: McKinsey Global Survey Results," *McKinsey Quarterly,* July 2011, (www.lonerganpartners.com/files/assets/docs/governance_since_the_economic_crisis.pdf); Brian Ballou, et al., "How Boards of Directors Perceive Risk Management Information," *Management Accounting Quarterly* 12, no. 4, Summer 2011, pp. 14–22.

45 McKinsey & Co., "Governance Since the Economic Crisis*,"* p. 2, Exhibit 1.

46 See Leech, "Risk Oversight, The High Cost of 'ERM Herd Mentality,'" pp. 5-6, discussing how traditional focus on accounting controls and compliance with Sarbanes-Oxley has not resulted in effective reporting for thousands of corporations.

47 See e.g., Ernst & Young, "Turning Risk into Results: How Leading Companies Use Risk Management to Fuel Better Performance," February 2012.

48 Gates, et al., "Enterprise Risk Management: A Process for Enhanced Management and Improved Performance," p. 28.

49 Gates, et al., "Enterprise Risk Management: A Process for Enhanced Management and Improved Performance," p. 36.

About the Author

Michelle Harner is a professor of law, associate dean for academic programs, and codirector of the Business Law Program at the University of Maryland Francis King Carey School of Law. She teaches courses in bankruptcy and creditors rights, business associations, business planning, corporate finance, and legal profession. Harner is widely published and lectures frequently on various topics involving corporate governance, financially distressed entities, risk management, and related legal issues. Her most recent publications appear or are forthcoming in the *Vanderbilt Law Review, Notre Dame Law Review, Washington University Law Review, Minnesota Law Review, Fordham Law Review* (reprinted in *Corporate Practice Commentator*), and *Arizona Law Review*. Harner currently serves as the Reporter to the American Bankruptcy Institute Commission to Study the Reform of Chapter 11. Previously, she was in private practice in the business restructuring, insolvency, bankruptcy, and related transactional fields, most recently as a partner at the Chicago office of the international law firm Jones Day.

Acknowledgements

The author would like to thank Jennifer Ivey-Crickenberger, Esq., UM Carey School of Law Business Law Fellow, and Angélica A. Matías, UM Carey School of Law J.D. Candidate, May 2013, for their valuable research and assistance.

About Director Notes

Director Notes is a series of online publications in which The Conference Board engages experts from several disciplines of business leadership, including corporate governance, risk oversight, and sustainability, in an open dialogue about topical issues of concern to member companies. The opinions expressed in this report are those of the author(s) only and do not necessarily reflect the views of The Conference Board. The Conference Board makes no representation as to the accuracy and completeness of the content. This report is not intended to provide legal advice with respect to any particular situation, and no legal or business decision should be based solely on its content.

About the Series Director

Matteo Tonello is managing director of corporate leadership at The Conference Board in New York. In his role, Tonello advises members of The Conference Board on issues of corporate governance, regulatory compliance, and risk management. He regularly participates as a speaker and moderator in educational programs on governance best practices and conducts analyses and research in collaboration with leading corporations, institutional investors and professional firms. He is the author of several publications, including *Corporate Governance Handbook: Legal Standards and Board Practices,* the annual *U.S. Directors' Compensation and Board Practices* and *Institutional Investment reports,* and *Sustainability in the Boardrooom*. Recently, he served as the co-chair of The Conference Board Expert Committee on Shareholder Activism and on the Technical Advisory Board to The Conference Board Task Force on Executive Compensation. He is a member of the Network for Sustainable Financial Markets. Prior to joining The Conference Board, he practiced corporate law at Davis Polk & Wardwell. Tonello is a graduate of Harvard Law School and the University of Bologna.

About the Executive Editor

Melissa Aguilar is a researcher in the corporate leadership department at The Conference Board in New York. Her research focuses on corporate governance and risk issues, including succession planning, enterprise risk management, and shareholder activism. Aguilar serves as executive editor of *Director Notes*, a bimonthly online publication published by The Conference Board for corporate board members and business executives that covers issues such as governance, risk, and sustainability. She is also the author of The Conference Board *Proxy Voting Fact Sheet* and co-author of *CEO Succession Practices*. Prior to joining The Conference Board, she reported on compliance and corporate governance issues as a contributor to *Compliance Week* and *Bloomberg Brief Financial Regulation*. Aguilar previously held a number of editorial positions at SourceMedia Inc.

About The Conference Board

The Conference Board is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance *and* better serve society. The Conference Board is a nonadvocacy, not-for-profit entity, holding 501(c)(3) tax-exempt status in the United States of America.

For more information on this report, please contact:
Melissa Aguilar, researcher, corporate leadership at 212 339 0303 or melissa.aguilar@conferenceboard.org

THE CONFERENCE BOARD, INC. www.conferenceboard.org

AMERICAS +1 212 759 0900 / customer.service@conferenceboard.org

ASIA-PACIFIC +65 6325 3121 / service.ap@conferenceboard.org

EUROPE/AFRICA/MIDDLE EAST +32 2 675 54 05 / brussels@conferenceboard.org

SOUTH ASIA +91 22 23051402 / admin.southasia@conferenceboard.org

THE CONFERENCE BOARD OF CANADA +1 613 526 3280 / www.conferenceboard.ca

© 2013 by The Conference Board, Inc. All rights reserved.
The Conference Board® and the torch logo are registered trademarks of The Conference Board, Inc.