



Director Notes



Corporate Culture and ERM

by Michelle Harner

The attitudes and actions of those viewed as leaders within a company (commonly referred to as “tone at the top”) help to define corporate culture and are critical to implementing a successful enterprise risk management (ERM) program. This *Director Notes* explores the challenges and benefits of creating a risk-aware corporate culture.

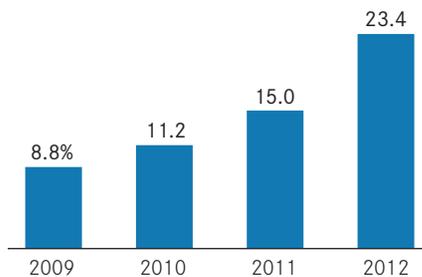
ERM as a Management Tool

Businesses, regardless of industry, are increasingly global, technology-driven, complex, and sensitive to market conditions. Boards of directors (boards) and senior management often are called upon to make critical decisions in a compressed time frame—decisions that may have a significant impact on the company, investors, employees, and the markets. These tasks are particularly challenging for directors who typically are not involved in the day-to-day operations of the company and must make decisions based on reports and data presented solely in the boardroom.¹ Those board meetings may not capture the true pulse of the company or the nuances and breadth of the decisions at hand.²

In that context, companies are increasingly using enterprise risk management (ERM) as a tool to better inform decision-making processes.³ ERM is a holistic approach to risk management that seeks to identify, assess, and manage known and emerging risks to the company and its objectives.⁴ It is grounded in strong channels of communication across the enterprise: a cross-functional initiative intended to manage more than financial risks.⁵ ERM, if properly implemented, can extract and synthesize relevant information to help boards and senior management understand more fully the issues and potential roadblocks to implementation of the company’s overall strategic plan. Rather than a snapshot, ERM facilitates a more vivid, robust, and in-depth study of alternative paths to success.



Chart 1
Percentage of organizations that report having a complete ERM process in place



Source: Mark Beasley, Bruce Branson, and Bonnie Hancock, "Current State of Enterprise Risk Oversight: Progress is Occurring but Opportunities for Improvement Remain," July 2012, p. 9.

Boards and senior management play critical roles in ERM.⁶ Boards oversee the process, determine the company's risk appetite, and help manage the company's risk profile within those parameters. Boards and senior management also set the company's culture, and these leaders are really the only individuals who can establish a risk-aware environment. Indeed, "tone at the top" has become in many respects synonymous with ERM.⁷

Corporate culture refers to a company's core values and objectives, as expressed through the attitudes and behavior of the board and senior management. Although the board alone cannot foster an effective ERM program, it can set the tone and exercise its oversight function in ways that facilitate meaningful risk management practices. The board is vital to creating a risk-aware and value-generating corporate culture.

Communicating What the Company Values

Commentators frequently invoke "tone at the top" when discussing ERM. It is more than a catch phrase—the concept is critical to implementing a successful risk management program. Tone at the top refers fundamentally to the attitudes and actions of those individuals viewed as leaders within a company. As risk management expert Douglas Brooks writes, "With culture, tone is critical, and the support must be behavioral as well as simply providing funding or resources.

It is up to leadership to effectively define the culture of the organization by encouraging, discouraging, and exhibiting certain behaviors."⁸ Accordingly, responsibility for setting this tone typically rests with the board and senior management.

Developing the correct tone and creating a risk-aware culture are difficult tasks. Research suggests, however, that they are well worth the time and effort because "[a] direct link exists between a company's culture and employee behavior."⁹ Commentators posit various guidelines to help boards and senior management change or improve their companies' culture.¹⁰ Although each company must find its own way, boards and managers who are committed to actively managing their companies' risk profiles within the parameters of carefully evaluated risk appetites, communicating that commitment to all employees, and adopting policies and incentive/compensation structures aligned with that commitment likely are moving in the right direction.

EXAMPLES

Good Tone at the Top, Poor Tone at the Top

Good tone at the top The company has policy statements and code of conduct which explicitly tell employees how they should behave in the company. The code of conduct applies to all employees, including top management. The importance of ethical behaviour is frequently highlighted by management through regular staff meetings. Employees are encouraged to communicate to their supervisors both "good news" and "bad news". Good job performance is well recognised. Top management always rewards appropriate behaviour and addresses inappropriate behaviour.

Bad tone at the top The company has policy statements and code of conduct which include general guidance of business ethics. The code of conduct applies to all employees, though top management seems not to be bound by the code of conduct. Employees read the code of conduct on the first day of their employment and seldom review it afterwards. The management team is autocratic. Employees are always afraid of delivering "bad news" to their supervisors. Good job performance is not always well recognised. Top management does not seem to care about or reward appropriate behaviour and address misbehaviour.

Source: Isabel Wang and Neil Fargher, "The Effect of Tone at the Top on Internal Auditors' Assessments of the Likelihood of Financial Misstatements," 2012, p. 28 (cbe.anu.edu.au/media/2429892/wangancaar.pdf).

A board can show its commitment to value creation through ethically sound business practices and approved risk-seeking strategies by, among other things, implementing an ERM program that clearly defines the company's risk appetite and reconciles that level of risk tolerance with the company's risk profile and strategic plan.¹¹ The board also needs to clearly communicate the company's approved level of risk-seeking activities to all employees, preferably through a written statement.¹² Commentators suggest that, in drafting a risk-appetite statement, boards should ensure that the established risk appetite:

- directly links to the organization's objectives;
- is stated precisely enough that it can be communicated throughout the organization, effectively monitored, and adjusted over time;
- helps with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risks (discussed in the next section);
- encourages alignment of people, processes, and infrastructure in pursuing organizational objectives within acceptable ranges of risk;
- keeps track of the competitive environment and considers shareholders' views in identifying the need to reassess or more fully communicate the risk appetite;
- recognizes that risk is temporal and relates to the time frame of the objectives being pursued; and
- recognizes that the organization has a portfolio of projects and objectives, as well as a portfolio of risks to manage, implying that risk appetite has meaning at the individual objective level and at the portfolio level.¹³

A company should also consider its risk appetite in designing its incentive and compensation structure. Some suggest that, "aligning executive compensation with the company's long-range objectives should limit executives' incentive[s] to make decisions that improve short-term metrics but increase the company's risk exposure."¹⁴ Adopting such an approach requires the board to consider what the company wants to value and reward through its incentive and compensation plans. Those objectives should complement and strengthen the board's efforts to establish the company's risk appetite and create a risk-aware culture.

To achieve this alignment, commentators suggest using nonfinancial metrics, such as product quality and customer satisfaction, in setting incentives and compensation.¹⁵

Integrating clawback provisions and linking stock option awards, at least in part, to nonfinancial metrics may also further the company's objectives.¹⁶ Admittedly, striking the appropriate balance in what at times might appear to be the conflicting objectives of value maximization and risk awareness can be challenging. Boards should remember, however, that this apparent conflict dissipates significantly if the company is working to align long-term value creation and risk minimization (or at least amelioration).

The Importance of "Walking the Talk"

As suggested above, a board decision to implement ERM and discuss risk awareness is not enough; the board also must "walk the talk."¹⁷ The behavior of the board and senior management must reflect the values pronounced in the risk-appetite statement and the internal and external communications regarding the ERM program.¹⁸ Although the production of these materials is an important initial step, the board and senior management must also be vested in the ERM process and open to the resulting flow of information. Asking employees to care about and prudently manage risk but not listening to or providing appropriate support for those risk-related discussions does little to foster a risk-aware culture.

Failure to listen and respond to risk-related concerns—whether generated through an ERM program or otherwise—also might expose the company to financial, operational, or reputational damage and the board to litigation and potential liability. For example, consider the significant trading losses sustained by JPMorgan Chase in the spring of 2012. Following a *New York Times* report that JPMorgan's trading loss from a bet on credit derivatives would far exceed earlier estimates and could total as much as \$9 billion,¹⁹ JPMorgan's stock price dipped 2.5 percent.²⁰ Moreover, reports suggested that "top investment bank executives raised concerns about the growing size and complexity of bets held by the bank's chief investment office as early as 2007."²¹ Investors predictably filed lawsuits against JPMorgan's board and management to recoup the losses.²²

This pattern is common—a company suffers losses from a risk event, investors or regulators allege that the board knew or had reason to know (i.e., red flags) of the risk and failed to address it, and litigation ensues.²³ Many companies, including AIG, Citigroup, Lehman Brothers, Worldcom, and Enron, have, faced such allegations.²⁴

In fact, the U.S. Senate Permanent Subcommittee on Investigations in its investigation of the Enron collapse concluded that: “By failing to provide sufficient oversight and restraint to stop management excess, the Enron Board contributed to the company’s collapse and bears a share of the responsibility for it.”²⁵

Some commentators suggest that red-flag allegations against boards are overused and often meritless. Michael Peregrine, for one, says, “Certainly, some of the cases involve instances where better oversight could have minimized some of the damage, [b]ut this allegorical love affair with ‘red flag’ references is harmful.”²⁶ Regardless of whether these commentators are correct or whether the board ultimately shows it has satisfied its fiduciary duties (discussed below), litigation is expensive, time consuming, and may harm the company’s and the board’s reputations. Accordingly, boards should ensure that their companies adopt and implement risk management programs that not only identify risks but also provide an effective process for the communication and consideration of risks. ERM offers a workable framework to help boards mitigate red-flag allegations and, perhaps more importantly, address any flags that pose real risk to the company or its objectives.

Of course, risk management should not drive all board or management decisions. Businesses are inherently entrepreneurial and, hence, involve the assumption of acceptable levels of risk. ERM, properly implemented, presents the opportunity for companies to consider and actively manage the “downside,” thereby setting the tone for profit maximization without taking imprudent risks. Advance consideration of those risks is always preferable to crisis-driven reactions to emerging events that might have been anticipated earlier.

The Importance of the Board’s Role from a Legal Perspective

The board, acting as a fiduciary for the company and its shareholders, owes certain fiduciary duties.²⁷ These generally include the duties of care and loyalty, but also more specific duties or obligations, such as good faith, disclosure, and oversight.²⁸ Although several fiduciary duties may be implicated, allegations of lax risk management typically invoke the board’s oversight duty, also referred to as the duty to monitor.²⁹

Courts generally defer to the board’s business judgment on matters concerning the company, including the structure and substance of the company’s compliance and monitoring programs.³⁰ As such, courts typically protect boards against oversight liability if a reasonable monitoring or reporting system is in place.³¹ Courts commonly articulate this standard as imposing liability only for “sustained or systemic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists.”³²

Courts have offered guidance on the types of conduct that might satisfy this standard. For example, evidence that the board knowingly disregarded risks or intentionally failed to monitor or oversee the company’s operations might suffice.³³ The critical element for most courts appears to be scienter, or evidence of the board’s knowledge or intent.³⁴ Plaintiffs have tried to prove scienter through evidence of red flags—issues raised but overlooked or ignored by the board. The particularized allegations and the types of alleged wrongful conduct needed to survive a motion to dismiss in duty to monitor litigation are found in *American International Group v. Greenberg*, *Louisiana Municipal Police v. Pyott*, and *In re Puda Coal, Inc. Shareholders Litigation*.³⁵

In the *AIG* case, a group of shareholders filed a derivative lawsuit on behalf of the company alleging wrongdoing by the chairman of the board, other directors and executive officers, certain other personnel, and the company’s accounting firm. The allegations included the intentional making of materially misleading financial statements, overstating the value of the corporation by billions of dollars, and engaging in conspiracies with competitors to rig the municipal derivative and general insurance markets.³⁶ More specifically, the plaintiffs alleged that the CEO and his “inner circle”—a small group of long-time executives who received lucrative compensation packages that were characterized as “rewards” from the CEO—directed widespread illegal conduct.³⁷

In the *Pyott* case, a shareholder brought a derivative action against individual directors of a pharmaceutical corporation after the company pled guilty to criminal misdemeanor misbranding and paid civil and criminal fines.³⁸ Notably, the court refused to grant a motion to dismiss, even after acknowledging the burden of proof to be high, because the board of directors had “discussed and approved a series of annual strategic plans” premised on illegal activity for at least a four-year period.³⁹

Finally, in the *Puda Coal* case, Chancellor Strine of the Delaware Chancery Court denied a motion to dismiss breach of fiduciary duty claims against independent directors where the directors allegedly did not know about unauthorized transfers of corporate assets in China.⁴⁰ Chancellor Strine explained, “[I]f you’re going to have a company domiciled for purposes of its relations with its investors in Delaware and the assets and operations of that company are situated in China that, in order for you to meet your obligation of good faith, you better have your physical body in China an awful lot.”⁴¹ As one commentator noted, “[the case] is a useful reminder to board members of Delaware corporations who need to be especially concerned about how they fulfill their oversight duties when the corporate operations or assets may be located in far-flung countries.”⁴²

Despite the *AIG*, *Pyott*, and *Puda Coal* cases, it remains difficult to establish breaches of a board’s duty to monitor, particularly in the context of business risks.⁴³ The honest and diligent board that has implemented a reasonable risk management or oversight program should garner protection.⁴⁴ That program further should include clear processes for the investigation and handling of risks identified or reported through the program. The more systematic the approach, the less likely that red-flag allegations will emerge or be entertained by the courts.

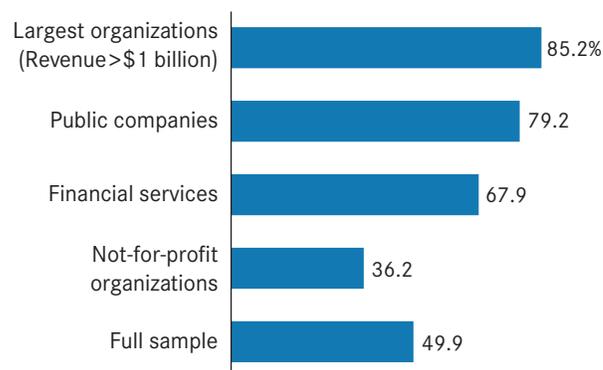
The Importance of the Board’s Role from an ERM Perspective

The board’s oversight duty should guide its role in ERM. The board cannot, and should not, be responsible for managing all risks or implementing all aspects of the ERM program. Rather, the board should take an institutional- or entity-level role in the program. For example, the board should participate in the design and rollout of the ERM program, take the lead in cultivating a risk-aware culture, set the company’s risk appetite, and align that with the company’s risk profile. Moreover, the board should remain involved in evaluating the company’s strategic risks, and monitor the implementation and functioning of the overall program.⁴⁵

According to an ERM survey published in July 2012,⁴⁶ “only 45.9 percent of the respondents in the full sample [over 600 executives] indicated that their boards have formally assigned risk oversight responsibility to a board committee.”⁴⁷

Chart 2

Percentage of organizations that formally report top risk exposures to the board at least annually



Source: Mark Beasley, Bruce Branson, and Bonnie Hancock, “Current State of Enterprise Risk Oversight: Progress is Occurring but Opportunities for Improvement Remain,” July 2012, p. 26.

This percentage was much higher for larger organizations, public companies, and financial services firms—80.7 percent, 82 percent, and 71.5 percent, respectively.⁴⁸ Similar trends were identified in questions concerning reports of the company’s top risks to the board and the integration of risk discussions with strategic planning. Approximately half of all respondents indicated a practice of producing such reports for the board on an annual basis and engaging in integrated discussions, but these percentages were, once again, much higher for larger organizations, public companies, and financial services firms.⁴⁹

The board should not try to micro-manage the ERM program. That type of oversight and responsibility should rest with management and risk owners at the unit, department, or other appropriate levels throughout the organization. However, a board can, take the following steps to enhance the company’s ERM program and ultimate performance.⁵⁰

Understand risks Work with management to understand the company’s risk profile, where the company’s critical risks are situated throughout the entity structure, and how those risks are interrelated.

Develop risk appetite Develop the company’s risk appetite (and related risk-appetite statement) and work with management and the appropriate professionals to set metrics to monitor the alignment of that risk appetite with the company’s risk profile.

Set clear expectations Establish clear expectations concerning risk management with management, risk owners, and others involved in the implementation and monitoring of the ERM program, and underscore those expectations in structuring incentives and compensation.

Know the plan Review management’s plans for implementing, monitoring, and communicating the ERM program and the company’s risk appetite throughout the company, ensuring well-defined channels of communication, expectations concerning risk management, and the consequences of actions exceeding the company’s risk appetite.

Obtain information Require periodic reports from management, risk owners, and others involved in the implementation and monitoring of the ERM program on the status of the program and the entity-level risks requiring board consideration and action.

Take action Integrate risk discussions with strategic planning and ensure that the company’s primary business objectives are communicated effectively throughout the company to facilitate similar integration at all levels of risk management.⁵¹

Notably, the survey referenced above found that only 37.1 percent of respondents attempted to integrate risk discussions with strategic planning and, in turn, consider “emerging strategic, market, or industry risks.”⁵² Yet this step of the ERM process is essential to long-term sustainability and value creation. Boards should encourage their companies to consider not only the risks they face today, but also those that might impede their progress tomorrow by embracing such an approach in their consideration of entity-level risks. Being vested in the process and leading by example can help boards cultivate a risk-aware culture and a meaningful ERM program.

Boards Play a Critical and Positive Role in ERM

An effective ERM program requires buy-in at all levels of the company, but that process starts with the board and senior management. The attitudes and behavior of the board and senior management (tone at the top) can trigger a positive (or negative) chain reaction throughout the company regarding risk management practices and their relationship to the company’s strategic objectives.

Boards considering reasons to implement ERM should examine the growing data suggesting a correlation between mature risk management practices and value creation, as well as the increasing scrutiny of risk management practices by courts and regulators.⁵³ In addition, implementing a process that fosters better information and communication concerning potential barriers to the company’s strategic objectives is simply good management. Many organizations and investors are urging companies to adopt ERM as best practice,⁵⁴ and as ERM processes continue to evolve, companies appear to be embracing this recommendation.⁵⁵

Accordingly, boards should take the time to understand ERM and its potential application to their companies. They also should appreciate that any ERM program will be only as successful as their involvement signals it should be. Tone at the top is more than a catch phrase; it is the genesis of a company’s culture and, consequently, necessary to establish a risk-aware and value-generating corporate environment.

Endnotes

- 1 Michael Useem, "How Well-Run Boards Make Decisions," *Harvard Business Review*, November 2006, pp. 130-131 (describing how companies are starting to develop more formal processes for figuring out which decisions should go to the board); and Martin Lipton, et al., "Risk Management and the Board of Directors," *Bank and Corporate Governance Law Reporter*, 45, no. 6, February 2011, p. 793 (noting that the board cannot and should not be involved in actual day-to-day risk management). See also Robert T. Miller, "The Board's Duty to Monitor Risk After Citigroup," *University of Pennsylvania Journal of Business Law*, 12, issue 4, August 2010, pp. 1166-1167 (arguing that the decision regarding what information should be presented to the board of directors is a business decision itself). All links listed in the report were last checked on May 6, 2013.
- 2 See, for example, Mark Beasley, Bruce Branson, and Bonnie Hancock, "Current State of Enterprise Risk Oversight: Progress Is Occurring But Opportunities For Improvement Remain," July 2012, p. 26 (noting how, for the full sample of survey respondents, organizations are more likely to report less than five risk exposures to the board or one of its committees). The report is available on the Poole College of Management website (http://poole.ncsu.edu/vol2/erm/ee/i/weblogs/research-documents/AICPA_ERM_Research_Study_2012_Final_Submission_July_16,_2012.pdf).
- 3 Beasley, Branson, and Hancock, "Current State of Enterprise Risk Oversight," pp. 9-10.
- 4 See, for example, PricewaterhouseCoopers, "Extending Enterprise Risk Management (ERM) to Address Emerging Risks," April 2009 (describing how organizations must refine their risk management processes to ensure that risks are "identified, assessed, and managed from strategic planning to day-to-day processes at all levels of the organisation"); and Martin F. Grace, et al., "The Value of Investing in Enterprise Risk Management," May 2010 (www.fox.temple.edu/cms/wp-content/uploads/2012/06/RichPhillips.pdf).
- 5 There are several frameworks for assessing ERM practices, including COSO Enterprise Risk Management—Integrated Framework, ISO 31000 Risk Management—Principles and Guidelines on Implementation, AS/NZ 4360 Risk Management Set, CAN/CSA-Q850; BS 31100 Code of Practice for Risk Management, and FERMA—A Risk Management Standards. See, for example, Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management-Integrated Framework: Executive Summary 1* 2004 (www.coso.org/documents/coso_erm_executivesummary.pdf) [hereinafter COSO Report]; Dorothy Gjerdrum and Mary Peter, "The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework," *Risk Management*, 21, March 2011 (https://na.theiia.org/standards-guidance/Public%20Documents/7-2-%20Article_on_ISO_for_Auditors_rev7-20.pdf) (comparing COSO and ISO frameworks). See also PricewaterhouseCoopers, "Extending Enterprise Risk Management (ERM) to Address Emerging Risks," pp. 11, 21 (describing how management tends to focus on financial and compliance risks and providing a table with sample emerging risks such as security, climate change, and health).
- 6 PricewaterhouseCoopers, "Extending Enterprise Risk Management (ERM) to Address Emerging Risks," p. 6 (describing the roles and responsibilities of the directors, officers, and other personnel in regard to ERM); and Lipton, et al., "Risk management and the Board," p. 793 (describing how directors should fulfill an oversight role, while the senior executives and risk managers design and implement the company's risk strategy).
- 7 Lipton, et al., "Risk Management and the Board," p. 794 ("The 'tone at the top' established by the board and the CEO shapes corporate culture and permeates the corporation's internal and external relationships."); John Brackett, "Corporate Culture: Creating Strong Guardrails for Governance and ERM," RSM International *Talking Points* March 2012, p. 2 (describing how internal auditors have for years referred to "tone at the top" in assessing a company); Larry Rittenberg and Frank Martens, "Enterprise Risk Management: Understanding and Communicating Risk Appetite," COSO, January 2012, p. 22; Ernst & Young, "Turning Risk into Results: How Leading Companies use Risk Management to Fuel Better Performance," February 2012, pp. 12 and 13; and Isabel Wang and Neil Fargher, "The Effect of Tone at the Top on Internal Auditors' Assessments of the Likelihood of Financial Misstatements" (<http://cbe.anu.edu.au/media/2429892/wangancaar.pdf>).
- 8 Douglas W. Brooks, "Creating a Risk-Aware Culture," in *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, eds. John Fraser and Betty Simkin (Hoboken, NJ: John Wiley & Sons Inc., 2010), pp. 87 and 93. See also Association of Insurance and Risk Managers, et al., "A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000," February 2010, p. 7 (observing that "[t]he initial component of the ISO 31000 framework is 'mandate and commitment' by the Board") The report, hereinafter referred to as "Requirements of ISO" is available on the Institute of Risk Management website (http://their.org/documents/SARM_FINAL.pdf).
- 9 Brackett, "Corporate Culture," p. 2; Ernst & Young, "Turning Risk into Results," p. 12. See also Grace, et al., "The Value of Investing in Enterprise Risk Management" (finding that "enterprise risk management improves firm operating performance").
- 10 See Tim Leech, "Board Oversight of Management's Risk Appetite and Tolerance," The Conference Board, Director Notes, 4, no. 23, December 2012, p. 2 (discussing COSO and ISO ERM frameworks and offering guidance on implementation based on, among other things, the National Association of Corporate Directors Blue Ribbon Commission report, *Risk Governance: Balancing Risk and Rewards*). See also Brackett, "Corporate Culture," p. 2; Ernst & Young, "Turning Risk into Results," p. 12; PricewaterhouseCoopers, "Extending Enterprise Risk Management"; and Protiviti, "Performance/Risk Integration Management Model – PRIM2," 2011, p. 6 (www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/PRIM2-Early-Mover-Analyzing-Strategic-Risk-Protiviti.pdf).
- 11 Stephen Gates, Jean-Louis Nicolas, and Paul L. Walker, "Enterprise Risk Management: A Process for Enhanced Management and Improved Performance," *Management Accounting Quarterly*, 13, Spring 2012, p. 36 (concluding that implementation of a structured approach to ERM results in improved performance, among other benefits); PricewaterhouseCoopers, "Extending Enterprise Risk Management," p. 16. ("The organisation should define tolerance levels for all key risks or risk categories identified... [because] [c]ertain emerging risks could put the organisation out of business, while others may present an opportunity to reshape the market.")
- 12 See Lipton, et al., "Risk management and the Board," p. 794 ("transparency, consistency and communication are key: the board's vision for the corporation, including its commitment to risk oversight, ethics and intolerance of compliance failures, should be communicated effectively throughout the organization); Rittenberg and Martens, "Enterprise Risk Management," 6-8 (discussing strategies for communicating risk appetite).
- 13 Rittenberg and Martens, "Enterprise Risk Management," p. 6.
- 14 ERM Initiative faculty and Lora Blackburn, "Aligning Risk Compensation and Executive Compensation" (www.poole.ncsu.edu/erm/index.php/articles/entry/aligning-executive-compensation).
- 15 Matteo Tonello, "The Role of the Board in Turbulent Times: Overseeing Risk Management and Executive Compensation: Pressure Points for Corporate Directors," The Conference Board, Executive Action 292, December 2008. See also the Corporate Compliance Committee, ABA Section of Business Law, "Corporate Compliance Survey," *The Business Lawyer*, 60, no. 4 August 2005, 1759, 1787 (noting that "[n]o employee will believe that a company values honesty and fair dealing if promotions

Endnotes (continued)

- and raises go to those who ‘meet the numbers’ by cutting corners and sharp dealing”); and Stephen M. Cutler, “Tone at the Top: Getting it Right, Speech at Second Annual General Counsel Roundtable,” December 3, 2004 (www.sec.gov/news/speech/spch120304smc.htm).
- 16 Tonello, “The Role of the Board in Turbulent Times,” p. 3. (“[Executive] performance should be assessed based on a combination of financial and extra-financial metrics.”)
 - 17 Brackett, “Corporate Culture,” p. 3; and Ernst & Young, “Turning Risk into Results,” p. 12 (discussing the importance of leadership and leading by example for successful risk management).
 - 18 Corporate Compliance Committee, ABA Section of Business Law, “Corporate Compliance Survey,” p. 1787; Brackett, “Corporate Culture,” p. 3; and Ernst & Young, “Turning Risk into Results,” p. 12.
 - 19 Jessica Silver-Greenberg and Susanne Craig, “JPMorgan Trading Loss May Reach \$9 Billion,” *New York Times*, June 28, 2012 (http://dealbook.nytimes.com/2012/06/28/jpmorgan-trading-loss-may-reach-9-billion/?_r=0).
 - 20 Aaron Smith, “JPMorgan Shares Fall on \$9 Billion Loss Report,” *CNNMoney*, June 28, 2012, (<http://money.cnn.com/2012/06/28/investing/jpmorgan-stock/index.htm>).
 - 21 Jessica Silver-Greenberg and Nelson D. Schwartz, “Red Flags Said to Go Unheeded by Bosses at JPMorgan,” *New York Times Dealbook*, May 14, 2012 (<http://dealbook.nytimes.com/2012/05/14/warnings-said-to-go-unheeded-by-chase-bosses/>).
 - 22 Bob Van Voris, “JPMorgan Shareholders Sue Dimon Over \$2 Billion Loss,” *Bloomberg*, May 16, 2012, (www.bloomberg.com/news/2012-05-16/jpmorgan-shareholders-sue-dimon-over-2-billion-trading-loss.html).
 - 23 See, for example, Anne Tucker Nees, “Who’s the Boss? Unmasking Oversight Liability Within the Corporate Power Puzzle,” *Delaware Journal of Corporate Law*, 35, no. 1, January 2010, p. 199, (discussing the common chain of events when companies experience significant financial loss – shareholders litigate, alleging inadequate oversight of risks); and Hillary A. Sale, “Monitoring Caremark’s Good Faith,” *Delaware Journal of Corporate Law*, 32, no. 3, 2007, 719, 734–735 (noting how apparent red flags have led to derivative litigation in several cases).
 - 24 See also Brenner v. Albrecht, No. C.A. 6514-VCP, 2012 WL 252286 (Del. Ch. Jan. 27, 2012) (noting shareholder derivative action on behalf of SunPower Corp. was due to failure to implement and to monitor an effective internal control system); In re Goldman Sachs Group, Inc. S’holder Litig., No. C.A. 5215-VCG, 2011 WL 4826104 (Oct. 12, 2011) (noting shareholder derivative action was based, in part, on a failure to properly monitor the company’s legal compliance program and the company’s compensation scheme for investment bankers); and Sherman v. Ryan, 911 N.E.2d 378, 394-95 (Ill. App. 2009) (noting shareholder derivative action on behalf of Aon Corp. was due to failure to supervise in the face of repeated “red flags”).
 - 25 U.S. Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations, *The Role of the Board of Directors in Enron’s Collapse* (Washington, DC: GPO, 2002) p. 59.
 - 26 Michael W. Peregrine, “Seeing Red Flags Where None Exist,” *New York Times Dealbook*, June 14, 2012 (http://dealbook.nytimes.com/2012/06/14/seeing-red-flags-where-none-exist/?_r=0).
 - 27 N. Am. Catholic Educ. Programming Found., Inc. v. Gheewalla, 930 A.2d 92 (Del. 2007); and Dodge v. Ford Motor Co., 204 Mich. 459, 507, 170 N.W. 668, 684 (1919); Model Business Corporation Act Annotated § 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, for example, *Gheewalla*, 930 A.2d at 101-103.
 - 28 *Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 369-70 (Del. 2006).
 - 29 *Stone*, 911 A.2d at 369-70. Risk management may already be highly relevant to the board’s duty to monitor due to the changing regulatory environment. See Michelle M. Harner, “Barrier to Effective Risk Management,” *Seton Hall Law Review* 40, issue 4, 2010, pp. 1323, 1330–1331 (discussing regulatory requirements of Sarbanes-Oxley and the New York Stock Exchange).
 - 30 See, for example, *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). See also *In re Citigroup Inc. S’holder Derivative Litig.*, 964 A.2d 106, 131 (Del. Ch. 2009). (“To impose oversight liability on the directors for failure to monitor ‘excessive’ risk would involve courts in conducting hindsight evaluations of decisions at the heart of the business judgment of directors.”)
 - 31 See *In re Caremark Int’l Inc. Derivative Litig.*, 698 A.2d at 971; *ATM-Kim Eng Fin. Corp. v. Araneta*, Civ. No. 489-N, 2006 WL 3783520 at *19-21 (Del. Ch. Dec. 21, 2006), *aff’d* 930 A.2d 928 (Del. 2007) (finding two members of the board breached of duty to monitor the disloyal and fraudulent conduct of another board member).
 - 32 See *Caremark*, 698 A.2d at 971.
 - 33 See, e.g., *Stone*, 911 A.2d at 369–70. (“Caremark articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls, or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.”) See also Donald A. Corbett and Daniel Roque, “Losses, but No Liability, for the Failure to Monitor Business Risk,” *Inside*, New York State Bar Association, 27, no. 3, Winter 2009, p. 9.
 - 34 See *Caremark*, 698 A.2d at 125, 123, fn. 47; *Citigroup*, 964 A.2d at 125; *Goldman*, No. C.A. 5215-VCG, 2011 WL 4826104 at *20 (Oct. 12, 2011); and *Brenner v. Albrecht*, No. C.A. 6514-VCP, 2012 WL 252286 at *5 (Del. Ch. Jan. 27, 2012).
 - 35 *Am. Int’l Group v. Greenberg*, 965 A.2d 763 (Del. Ch. 2009), *aff’d* 11 A.3d 228 (Del. 2011) (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); *La. Mun. Police Empls Ret. Sys. v. Pyott*, 46 A.3d 313 (Del. Ch. 2012) (denying motion to dismiss, among other things, duty to monitor claims); and *In re Puda Coal, Inc. Stockholders Litigation*, C.A. No. 6476-CS (Del. Ch. Feb. 6, 2013) (bench ruling) (denying motion to dismiss breach of fiduciary duty claims against independent directors in case involving oversight of assets in foreign jurisdictions). See also *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).
 - 36 *Greenberg*, 965 A.2d at 774-75.
 - 37 *Greenberg*, 965 A.2d at 774-75.
 - 38 *Pyott*, 46 A.3d at 317-21.
 - 39 *Pyott*, 46 A.3d at 42, 352-53.

Endnotes (continued)

- 40 *In re Puda Coal, Inc. Stockholders Litigation*, C.A. No. 6476-CS (Del. Ch. Feb. 6, 2013) (bench ruling), transcript available at www.delawarelitigation.com/files/2013/02/puda-case.pdf (last visited May 6, 2013). See also Kevin LaCroix, “Delaware Chancery Court: A Sweeping Revision of Outside Directors’ Foreign Operations Oversight Responsibilities?” D&O Diary Blog, February 27, 2013 (www.dandodiary.com/2013/02/articles/shareholders-derivative-litiga/delaware-chancery-court-a-sweeping-vision-of-outside-directors-foreign-operations-oversight-responsibilities); and Tariq Mundiya, “Independent Director Duties of Delaware Corporations with Foreign Operations,” Harvard Law Blog, February 23, 2013 (blogs.law.harvard.edu/corpgov/2013/02/23/independent-director-duties-of-delaware-corporations-with-foreign-operations). For background on underlying investigation, see Joshua Gallu and Karen Gullo, “Puda Coal Executives Stole Company Assets, SEC Alleges in Suit,” Bloomberg News, February 24, 2012 (www.businessweek.com/news/2012-02-24/puda-coal-executives-stole-company-assets-sec-alleges-in-suit.html).
- 41 *In re Puda Coal, Inc.* C.A. No. 6476-CS (Del. Ch. Feb. 6, 2013).
- 42 Francis Pileggi, “Delaware Board’s Fiduciary Duty of Oversight for Foreign Operations,” Delaware Corporate & Commercial Litigation Blog, February 19, 2013 (www.delawarelitigation.com/2013/02/articles/chancery-court-updates/fiduciary-duty-of-oversight-for-foreign-operations-of-us-company).
- 43 *Citigroup*, 964 A.2d at 125 (quoting *Caremark*, 698 A.2d at 967) (“[d]irector liability based on the duty of oversight ‘is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment’”).
- 44 See, for example, *Stone*, 911 A.2d 362, 373 (“[d]irectors’ good faith exercise of oversight responsibility may not invariably prevent employees from violating criminal laws, or from causing the corporation to incur significant financial liability, or both”).
- 45 See, for example, PricewaterhouseCoopers, “Extending Enterprise Risk Management,” p. 25 (“To improve their risk resilience, organisations are challenged to revisit, innovate, and refine [their ERM programs]... to ensure that... [a]ssessment of these risks occurs periodically, ... [r]isk responses are determined or revised as necessary... [, and] [a]dequate monitoring mechanisms are developed and tracked routinely.”); and Rittenberg and Martens, “Enterprise Risk Management,” p. 2. (“Once risk appetite is communicated, management, with board support, needs to revisit and reinforce it. Risk appetite cannot be set once and then left alone.”)
- 46 Beasley, Branson, and Hancock, “Current State of Enterprise Risk Oversight.”
- 47 Beasley, Branson, and Hancock, “Current State of Enterprise Risk Oversight,” p. 25.
- 48 Beasley, Branson, and Hancock, “Current State of Enterprise Risk Oversight.”
- 49 Beasley, Branson and Hancock, “Current State of Enterprise Risk Oversight,” p. 26.
- 50 Lipton, et al., “Risk Management and the Board,” pp. 796-797. (Other appropriate considerations include, reviewing the steps taken by management to ensure adequate independence of the risk management function and the processes for resolution and escalation of differences that might arise between risk management and business functions, reviewing with management the design of the program to include discussions of potential coverage gaps or issues with lines or reporting; and reviewing the qualifications and background of senior risk officers and personnel policies applicable to risk management.)
- 51 Lipton, et al., “Risk Management and the Board,” 794 (noting risk management should be viewed as “an integral component of the firm’s corporate strategy, culture and business operations”); Leech, “Board Oversight of Management’s Risk Appetite,” pp. 4, 6 (discussing how many organizations fail to identify predictable or expected risks that may affect their strategic plan); COSO Report, p. 3 (“Achievement of strategic objectives and operations objectives, however, is subject to external events not always within the entity’s control; accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.”); and Association of Insurance and Risk Managers, et al., “A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000,” p. 6 (“Risk management must be integrated into the culture of the organisation and this will include mandate, leadership and commitment from the Board. It must translate risk strategy into tactical and operational objectives, and assign risk management responsibilities throughout the organisation.”).
- 52 Beasley, Branson, and Hancock, “Current State of Enterprise Risk Oversight,” p. 4. (“Less than one-third [of survey respondents] have ‘mostly’ or ‘exclusively’ articulated the organization’s appetite for or tolerance of risks in the context of strategic planning. Just over 15 percent believe ‘mostly’ or ‘extensively’ that the organization’s risk management process is a proprietary strategic tool that provides unique competitive advantage.”)
- 53 See, for example, Gates, Nicolas, and Walker, “Enterprise Risk Management,” pp. 28-29 (discussing how ERM is useful in the face of regulatory pressures and also creates value); Leech, “Board Oversight of Management’s Risk Appetite,” p. 2 (noting that ERM is implicated in multiple regulatory regimes and creates shareholder value); and Lipton, et al., “Risk Management and the Board,” (discussing ERM as a means of fulfilling director duties in the face of the regulatory climate).
- 54 Leech, “Board Oversight of Management’s Risk Appetite,” pp. 2-3 (discussing the Sarbanes-Oxley Act as well as recommendations by the SEC, the National Association of Corporate Directors, the International Corporate Governance Network, the Canadian Institute of Chartered Accountants, and the Institute for Internal Auditors); PricewaterhouseCoopers, “Extending Enterprise Risk Management,” p. 3 (discussing the ERM standard laid out by Standard & Poor’s and also the ERM recommendations of the United States’ “Implementing Recommendations of the 9/11 Commission Act of 2007.”); and Michael Alix, Senior Vice President of the Federal Reserve Bank of New York, 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) (describing how the Counterparty Risk Management Policy Group and the “Senior Supervisors Group” have called for improvements in risk governance and financial firms).
- 55 Beasley, Branson, and Hancock, “Current State of Enterprise Risk Oversight,” p. 9 (indicating there has been a steady increase in the number of organizations embracing ERM over time and noting that for the full sample of respondents, the percentage has increased from 8.8 percent in 2009 to 23.4 percent in 2012).

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*), *Florida Law Review*, 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.

Acknowledgments

The author would like to thank Jennifer Ivey-Crickenberger, Esq., UM Carey School of Law Business Law Fellow, and Angélica A. Matías, J.D., UM Carey School of Law, 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, Sustainability in the Boardroom*, and the forthcoming *Risk Oversight Handbook*. 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 coauthor 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