

ERM—It's BAAACK! Fiduciary Duty and Enterprise Risk Management

By Michael W. Peregrine, McDermott Will & Emery LLP, Chicago, IL

I'll admit it. For the longest time, when I heard the phrase "Enterprise Risk Management," my eyes glossed over, and I mentally turned the page. *Next Topic, Please!* Maybe this works for Fortune 100 companies, but for nonprofit hospitals and health systems? *I don't think so.* And, I'm not going to bug my clients about it—they have enough, legitimate issues to be concerned with—right?

Well, I was wrong. Big time.

Enterprise risk management has emerged from the embers of the recession to become an increasingly recognized component of the board's fiduciary oversight obligation. "ERM" concepts apply across industry lines, without regard to whether a company is organized on a for-profit or nonprofit basis, is publicly held, closely held, or charitable in nature. "Best practice"? If not quite yet, then certainly soon. Regulators, rating agencies, and commercial policy groups (among other third parties) are leading the charge for the presence of a board-level ERM function—both as a reaction to prior corporate excesses, and as a prophylactic against future disabling risks. The benefits of managing against potentially devastating economic and corporate risks accrue to all commercial enterprises, including those in healthcare. Thus, it is more and more the "smart play" for nonprofit hospitals and health systems to incorporate some form of ERM function within the board's overall oversight activities. This is particularly the case for financially and organizationally sophisticated systems, which are often compared with their peers in the public company sector for regulatory and governance purposes.

What It Is

ERM concepts developed as a means by which corporate boards could improve their comprehensive oversight of risk management. ERM is reliably defined as "a process":

1. Effected by an entity's board, management, and personnel;
2. Applied in a strategy setting;
3. Applied across the enterprise;
4. Designed to identify potential events that may affect the entity;
5. Designed to manage risks to be within the company's risk appetite;
6. Able to provide reasonable assurance regarding achievement of entity objectives;
7. Geared to the achievement of objectives in one or more separate but overlapping categories—it is a means to an end, not an end in itself.¹

The general view is that ERM should not be perceived as a separate and distinct corporate infrastructure, but rather as

a means for incorporating more comprehensive risk management concepts within pre-existing financial and non-financial control mechanisms.² From a high-level perspective, these risks range from the obvious (e.g., compliance, operational, market, financial, fraud, information technology, health and safety) to the less obvious (e.g., political, reputational, intellectual property, product liability, employment, disaster, environmental). The goal of an ERM program is to provide corporate governance with a profile of the company's most material risks, so that the board may properly consider the relationship of those risks to corporate operations.³

What's Changed?

The genesis of ERM was the corporate responsibility environment in the post-Enron, Sarbanes-Oxley era, with its broad focus on governance oversight, management accountability, financial integrity, and concentration on internal controls. While the nonprofit healthcare sector generally adhered to core Sarbanes principles and sharpened board and financial management practices, the benefits of additional, special risk management mechanisms were neither obvious nor persuasive.

Developments over the past two years have changed all that. ERM has received a strong "second wind" through a combination of factors: (a) the scope, length, and breadth of the recession and the failure of industry to predict and adapt to its impact on all sectors of commerce; (b) government intervention with failing companies (e.g., TARP); (c) the sense that inappropriate, unsupervised corporate risk taking contributed to the economic damage; (d) an increased focus on the director's duty of care, particularly in connection with the development of post-recession corporate strategy; and (e) emerging federal regulation that mandate increased consideration, and disclosure, of internal risk management activities. Among these factors, several stand out for health industry attention:

» *Public Policy Formation:* Within the last year, two influential commercial policy organizations, The Conference Board and the National Association of Corporate Directors, each have published a substantial white paper arguing in favor of more focused ERM activity: "The fallout from the financial crisis is creating greater demands on boards of directors and senior executives to strengthen risk management practices, and this trend is no longer confined to banks and other financial institutions."⁴ These white papers provide a series of ERM implementation recommendations and warn against a false sense of security with respect to the adequacy of existing ERM processes.

» *Regulatory Direction:* New Securities and Exchange Commission (SEC) Final Rules (effective February 28, 2010) revise the compensation and corporate governance disclosure requirements applicable to public companies to incorporate several specific ERM-related provisions, among other new requirements.⁵ One of the most significant of the rules is that which requires companies to disclose how enterprise risk is taken into consideration with respect to determining executive compensation practices and policies. The disclosure obligation is triggered to the extent that the risk associated with such practices and policies is “reasonably likely to have a material adverse effect” on the company.⁶

In any related disclosure, the company is obligated to disclose its approach for balancing appropriate risk taking, and managing/mitigating excessive risk taking that may jeopardize the entire organization. Another significant new rule is that which requires disclosure of the extent of the board’s risk oversight efforts. In particular, the SEC seeks disclosure of the manner in which the board is made aware of the material, operational, and reputational risks confronting the company. This is consistent with corporate governance standards of the New York Stock Exchange, which require that the audit committees of listed companies maintain basic risk assessment and management oversight responsibilities.⁷

Along similar lines, Internal Revenue Service (IRS) Commissioner Douglas Shulman recently encouraged corporate directors to focus more closely on exercising oversight with respect to corporate tax risks and tax strategies.⁸ Commissioner Shulman made specific reference to the potential for material weaknesses in internal controls related to taxes, the financial and restatement risks presented by tax strategies, and the reputational risks associated with aggressive corporate tax strategies.⁹

» *Focus on Oversight Duty:* Over the last year, there also has been increased attention to the director’s fiduciary duty of oversight, which is at the core of ERM principles. For example, in an important decision, the Delaware Chancery Court concluded that a duty to oversee business risk exists under Delaware law, but that a plaintiff has an extraordinary burden in order to prevail on a related claim.¹⁰ Specifically, the claim would need to allege that the board completely failed to establish a business performance oversight system, failed to monitor that mechanism on a regular basis, or intentionally ignored a “red flag”—a difficult burden, indeed.¹¹ In so doing, the court expanded upon the traditional *Caremark* analysis with which healthcare counsel are familiar, in the context of board obligation to oversee corporate compliance plans (*see* discussion below).

Enterprise risk management has emerged from the embers of the recession to become an increasingly recognized component of the board’s fiduciary oversight obligation.

The Fiduciary Connection

From a fiduciary duty perspective, ERM concepts are grounded in the fundamental “oversight obligation” under the duty of care. This obligation pertains to the board’s activity in overseeing the day-to-day activities of the corporation—as opposed to the exercise of diligence with respect to a particular decision (for which business judgment rule protection may be available). In oversight situations, courts historically apply a “gross negligence standard,” finding breach only where a director has demonstrated a pattern of inattention or failure to respond to matured issues of which a prudent director would take notice.

Healthcare lawyers are familiar with the duty of oversight as it has been applied to articulate the board’s obligation to implement and exercise oversight over the corporate compliance program. The seminal *Caremark* decision concluded that a director’s oversight obligation includes a duty to attempt in good faith to assure that (1) a corporate information and reporting system, which the board concludes is adequate, exists; and (2) this system is sufficient to assure that appropriate information regarding organizational compliance with applicable laws will come to the board’s attention in a timely manner and in an ordinary course. The level of detail that is adequate for such an information and reporting system is a matter of the board’s business judgment.¹² *Caremark* and its progeny (through *In re Citigroup*) establish a high burden for director oversight liability in this context: that the directors either (a) 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.¹³ Thus, fiduciary liability exposure arises only upon a showing that the directors knew they were not discharging a fiduciary obligation; i.e., failing to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their responsibili-

Analysis

ties.¹⁴ The *Citigroup* decision, discussed above, drew a critical distinction between oversight liability with respect to failing to monitor and manage legal and compliance risks (requiring a high burden of proof) and with respect to failing to monitor and manage business risks (requiring an *even higher* burden of proof).

How to Implement

The various public policy white papers recommend at least a five-step approach by which a board might evaluate the sufficiency of existing internal ERM controls: *First*, evaluate the quality of risk information the board currently receives from executive staff; *Second*, work with executive staff to increase board awareness of the totality of the business risks confronting the company; *Third*, evaluate executive management's process to evaluate these risks; *Fourth*, assess the effectiveness of existing risk management procedures; and *Fifth*, seek out risk management related feedback from employees (other than the most senior members of executive management) involved in existing risk management programs.¹⁵ The white papers also prompt the board to consider how much tolerance it may have for variances from its core risk appetite, and encourage the board to be proactive in controlling the information flow on risk matters.¹⁶ Ultimately, the standard by which existing processes should be evaluated is whether they are sufficient to provide the board members with an understanding of the organization's risk profile, from which they may effectively exercise their related oversight obligations.

Structural Speed Bumps

In advising health system clients on ERM review and implementation, counsel should be mindful of at least four governance-related issues that experience suggests may present particular challenges:

- » *Industry Specific*: an effective ERM process for a nonprofit hospital or health system will be one that is industry specific and not an "off the shelf," generic version. An increasing number of board members may be working with risk management systems within their own business enterprises, but the specific processes used and elements of risk may be unsuitable for hospitals and health systems. Obvious unique features of a nonprofit hospital/health system ERM process will include (1) the solvency of the healthcare financing system; (2) emerging financial and strategic issues arising from the Patient Protection and Affordable Care Act (PPACA); (3) operating and legal issues associated with delivery/quality of care and clinical research matters; and (4) pressures on federal and state income and property tax exemptions, to name only a few.
- » *Board Responsibility*: the consensus of most commentaries and white papers (as well as the inference from emerging federal regulation) is that ERM responsibility rests with

In the post recession, heavily regulated, PPACA-centric environment in which nonprofit healthcare currently functions, the establishment of a dedicated risk management reporting and monitoring function makes good sense.

the full board, and not a subset or committee thereof. The temptation exists to assign ERM oversight to the audit committee, because its charter typically incorporates oversight of financial risk management as well as audit matters. Also, the perception is that audit committee members possess specialized risk-based expertise that makes them well-suited to address all types of oversight activity. All of this is true. Yet, the concern is that the audit committee will quickly become a "dumping ground" for all forms of risk-related duties and activities. This is particularly the case where responsibility for compliance plan oversight is already assigned to the audit committee. To locate ERM responsibility with the audit committee risks overloading with duties the members of a key committee. It also undermines the basic theme that responsibility for risk management fundamentally resides at the full board. Indeed, some of the larger and more sophisticated hospitals and health systems will consider locating ERM responsibility within a separate committee with board delegated powers, dedicated to risk management. Of course, the related challenge will be to assure horizontal coordination between risk management, audit, and corporate compliance oversight functions.

- » *Protect Compliance*: a significant concern with ERM implementation is the extent to which it may serve, intentionally or unintentionally, to reduce the prominence of the existing internal corporate compliance infrastructure. In an industry as heavily regulated as healthcare, it is hard to imagine a risk that is the equal to, or more prominent a concern, than risk related to legal compliance. Some board members who are strong advocates of an enhanced ERM process may not come from an industry where corporate compliance is as fundamental a concern as in healthcare.

Analysis

In the zeal to adopt prudent ERM processes, caution must be exercised not to distract board, committee, executive management, or senior staff focus—or resources—from the traditional and emerging corporate compliance risks. This is particularly the case with increased regulatory enforcement arising out of the specific provisions of the PPACA. In an effective health industry ERM program, all material identified risks are significant, but corporate compliance is more significant than the others.

» *Management v. Governance*: whether the ERM push comes from the board, or from management, it is vitally important to recognize the separate and distinct roles that each plays in the process. Clearly, it is the board that has the ultimate oversight responsibility for the development of corporate strategy and for the development and implementation of ERM processes. In both regards, the board is expected to consider the specific recommendations and directions contributed by the executive management team. More fundamentally, it is the responsibility of the executive management to identify for board consideration the core risk issues at the heart of an organization's ERM process, to effect the implementation of the specifically designed ERM program, and to regularly report to the board or key committee on the status of such core risks; in other words, to make it work. The board should refrain from "getting into the weeds" of risk management. Rather, it should work closely with senior executive leaders to create a reporting relationship that is designed to provide the board and its risk-related committees with the information they need to have in order to exercise their oversight responsibilities.

Conclusion

I was wrong. I admit it.

In the post recession, heavily regulated, PPACA-centric environment in which nonprofit healthcare currently functions, the establishment of a dedicated risk management reporting and monitoring function makes good sense. Furthermore, such a function is entirely consistent with the board's duty of care-based oversight function—something that recent case law, emerging federal regulation, and several prominent corporate policy white papers have clearly recognized.

Is it thus "best practice" for a board to direct the implementation of an ERM process? *No—I'm not ready to go there yet.* The concept is not so mature as to essentially constitute a standard of conduct, against which board practices would be judged. We are not remotely to the point where the absence of an ERM process creates board liability exposure, as might be the case if, e.g., the board knowingly declined to implement a corporate compliance and reporting program for the organization.

Where I come out is that the board should recognize that its oversight obligation includes monitoring all types of corporate risk—principally those relating to legal/corporate compliance, but also those other business risks that could have

a material effect on corporate operations and on the pursuit of the corporate mission. In that regard, the board should at least be having internal conversations on how best to oversee such risks, and should be seeking the advice of executive leadership on the most effective process to do so. ☐

Michael W. Peregrine (mperegrine@mwe.com) is a partner in the law firm of McDermott Will & Emery LLP and is based in the Firm's Chicago, IL office. He focuses his practice in the representation of nonprofit corporations in connection with governance, corporate structure, executive compensation, tax, and change-in-control matters. Mr. Peregrine is outside governance counsel to many leading nonprofit corporations. He has served as special counsel in connection with numerous confidential internal reviews and investigations. He also has substantial experience with complex business transactions, having advised nonprofit clients on over 85 separate mergers, acquisitions, and dispositions. Mr. Peregrine was named an AHLA Fellow in 2006, and is a frequent author and speaker on legal topics affecting tax exempt, nonprofit corporations.

Endnotes

- 1 Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framework*, Sept. 2004, available for purchase at www.coso.org/guidance.htm, Executive Summary, available at www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf. See also The Conference Board, *Adapting to Regulatory Developments and Emerging Practices*, available at www.conferenceboard.org (Conference Board 2009 Report); The Conference Board, *The Role of U.S. Corporate Boards in Enterprise Risk Management* (Conference Board 2006 Report), available at www.conference-board.org/publications/describe.cfm?id=1190 (published just before the commencement of the recession, this particular white paper has proven notably prophetic).
- 2 Conference Board Report 2009, *supra* note 1, at p. 10.
- 3 Lipton, Neff, Brownstein, Rosenblum, Emmerich, Niles, and Walker, *Risk Management and the Board of Directors*, *Corporate Governance Advisor* March/April 2010, Volume 18, No. 2.
- 4 Conference Board 2009 Report, *supra* note 1, at p. 1; see also National Association of Corporate Directors Blue Ribbon Commission Report, *Risk Governance: Balancing Risk and Reward*, www.nacdonline.org (NACD Report).
- 5 74 Fed. Reg. 68334 (Dec. 23, 2009), available at www.sec.gov/rules/final/2009/33-9089.pdf.
- 6 *Id.* See also McDermott Will & Emery White Paper, *Effects of the New Compensation and Corporate Governance Rules on the 2010 Proxy Season*, dated Jan. 5, 2010, available at www.mwe.com/info/news/wp0110a.pdf.
- 7 Final NYSE Corporate Governance Rules, available at www.nyse.com/pdfs/finalcorpgovrules.pdf.
- 8 IRS Commissioner Douglas Shulman, Prepared Remarks, National Association of Corporate Directors Governance Conference, Oct. 19, 2009, available at www.irs.gov/newsroom/article/0,,id=214451,00.html.
- 9 *Id.* In addition, several legislative proposals to restructure the banking/finance system incorporate ERM-related provisions.
- 10 *In re Citigroup Inc. Shareholder Derivative Litig.*, 964 A.2d 106 (Del. Ch. 2009).
- 11 *Id.* Gentile and Christensen, *In re Citigroup: The Birth Announcement and Obituary of the Duty of Business Performance Oversight*, *Bloomberg Law Reports—Corporate Law*, Vol. 3, No. 19 (2009).
- 12 *In re Caremark Int'l Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).
- 13 *Stone v. Ritter*, 911 A.2d 362, 370. (Del. Ch. 2006).
- 14 *Id.*
- 15 See, e.g., The Conference Board 2009 Report, *supra* note 1.
- 16 See, e.g., NACD Report, *supra* note 4.