New York Law Journal
Corporate Governance
WWW.NYLJ.COM
An ALM Publication
MONDAY, NOVEMBER 28, 2011

The Increasing Significance of **Enterprise Risk Management**

BY ISAAC E. DRUKER

PROMINENT SCANDALS involving three major U.S. publicly traded corporations about a decade ago, resulting from fraudulent accounting practices and executive corruption, raised urgent questions about the ability of corporate boards of directors to "mind the store"—and, in turn, impelled consideration of how better to deploy effective risk management techniques and assign responsibility for them.

More recently, during the financial liquidity crisis of 2008-2009, excess leverage and counterparty solvency issues in derivative and securities trading led to the "bail outs" of major financial institutions—and a fresh round of introspection regarding risk management.

Enron Corporation, Tyco International and WorldCom were each the victim of elaborate schemes. For Enron, the key issues were excessive use of "special purpose" off-shore entities, which enabled the concealment of billions in losses and mounting debt; the carrying of assets at grossly inflated values; and other questionable accounting practices. In the case of Tyco, its former Chairman and CEO and former CFO were found to have stolen in excess of $150 million from the company, which they claimed was compensation approved by the board. The board and former directors and officers became the objects of much litigation.

ISAAC E. DRUKER *(idruker@andersonkill.com) is a shareholder in the New York office of Anderson Kill & Olick and co-chair of the firm's Captive Insurance Group. He concentrates his practice on corporate, commercial and financial matters, including mergers and acquisitions; international and domestic business, investment and financial transactions; captive insurance; project finance; international and domestic joint ventures; and distribution, licensing and general commercial agreements.*


ISTOCK

The WorldCom scandal revealed other problems: fraudulent characterizing of certain operating expenses as capital expenditures so as to improve earnings, and board approval of more than $400 million in loans and guaranties to its CEO, to enable him to respond to margin calls rather than sell his WorldCom stock into an already declining market. These practices contributed to material loss of stockholder value and the ultimate liquidation of the enterprise.

Each of these debacles raised key questions as to safeguards that might have prevented these kinds of corporate fraud. Sophisticated, experienced boards apparently either lacked the tools to exercise adequate oversight or were not inclined to exercise their responsibilities to shareholders. Such boards did not exercise their "fiduciary duties" so as to uncover systematic accounting frauds perpetuated over many years or uncover potentially specious activities by their senior managements. The boards purportedly "on the watch" as the various cases grew and unfolded were later ignominiously dismissed and became the subjects of protracted litigation, while criminal sanctions were brought against certain members of senior management.

More recently, the liquidity crises that led to the failures, mergers or bail outs of the likes of Lehman, Merrill Lynch and AIG raised many issues as to the care with which management of these institutions, and others, systematically evaluated their exposures in the areas of, inter alia, mortgage-backed loans and collateralized debt obligations. What oversight was exercised by the respective boards, what risk management techniques should have been in place to raise early warning flags?

Enterprise Risk Management (ERM) implies much more than disaster contingency planning or establishing methods for discovery of dubious accounting practices and high risk short-term stock price manipulation. It requires that risk evaluation be incorporated into decision-making for all vulnerable areas of the subject business, and that the risk management functions are current agenda items for every board. Legislation, regulation, and market experience have all urged the incorporation of ERM as a matter of good corporate governance and an element of the fiduciary responsibility of boards and senior management to the business owners. In particular, the growth in governance practices of assignment of risk oversight responsibility for specific areas of corporate activity to a particular director or a "Risk Oversight Committee" of the board—so-called "portfolio responsibilities"—should result in improved initiation of appropriate analyses, pro-active strategies and preemptive planning. Not surprisingly, we will see that ERM also has an important place in the management of privately held companies. We will also describe how captive insurance companies can contribute importantly to the ERM function.

Evolution of ERM

The ultimate concern of enterprise risk management is the protection of the enterprise's core assets and therefore of shareholder value. During recent years, the discipline of ERM has become increasingly professionalized, with an emphasis on developing systems, procedures and structures, including the use of sophisticated metrics to analyze, calculate and monitor a company's exposures. More traditional areas of focus include incidence of factory plant-floor injuries, product safety/product liability issues, integrity of financial reporting, customer credit-worthiness, regulatory compliance, and often certain requirements imposed by insurance carriers. In the last decade, disaster contingency planning, terrorism risk and cyber risk have gained considerable attention.

However, ERM is not merely a program for risk avoidance. One of the major themes currently appearing in corporate governance writings relates to the integration of ERM techniques into long term strategic planning for sustainable growth. The thinking extends even to the following: what products are in the pipeline, where do they stand in relation to competitive offerings now and at projected time of introduction, what happens if the next "big hit" fails, what are potential alternatives? How does management compensation align with the pursuit of long term value growth and avoidance of short term stock price-driven strategies? What can be learned from the accounting scandals of a decade ago for detection of fraudulent accounting practices, and/or use of off-shore special purpose vehicles and similar "accounting" techniques?

ERM now entails taking a pro-active approach in every relevant sector of the business: analysis of prospective vulnerability ("key risk indicators"), the speed with which certain events will impact the ongoing company ("risk velocity"), the significance of the impact, an understanding of key underlying causes, consideration of curative or pre-emptive measures, and installation of structures and procedures to provide early alerts to senior management so as to enable rapid response.

In addition, it appears that integration of ERM with strategic goal-setting and planning enables the board and senior management to better understand risks inherent in a particular course of action, consciously decide on the degree of acceptable risk, and articulate the response to be taken in the event risk parameters are exceeded. Conscious application of enterprise risk analysis and risk management techniques enables the board and senior management to better prioritize opportunities from a risk-reward point of view. It is tempting to speculate to what extent aggressive adoption of such strategies might have averted the liquidity crisis and near-collapse of AIG, in part a consequence of the acts of its London office, which issued hundreds of billions of dollars of mortgage insurance derivative contracts.

Enterprise Risk Management requires that risk evaluation be incorporated into decision-making for **all vulnerable areas** of the subject business, and that the risk management functions are **current agenda items** for every board.

Corporate Governance

The Sarbanes-Oxley Act of 2002 (SOX), the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2011 (Dodd Frank) and the report of the New York Stock Exchange (NYSE) Commission on Corporate Governance, released in September 2010, are good milestones in the evolution of governance standards and principles and their increased acceptance by various constituencies in recent years. Several early SOX objectives, in response to issues at the heart of the Enron and WorldCom scandals, were improved financial disclosure, enhancing the function of internal audit by installing the independent audit committee, strengthening the role of the independent director and protection of whistlebowers. In addition, SOX §304 required certain executives to repay inflated compensations computed on the basis of financial information subsequently restated, an approach followed and broadened by §954 of Dodd-Frank.

The NYSE Commission, with its composition drawn from company management, boards, investors, financial institutions, and other experts, was designed to set out "state of the industry" concepts. Its emphasis on the utility of risk management concepts is evident in a number of principles adopted.

Principle No. 1 set out in the NYSE Commission's report notably emphasizes building long-term sustainable growth in shareholder value versus short term relatively high-risk action, taken to "bump up" share price but possibly jeopardizing long-term objectives. Aligning management compensation to long term value growth would be a desirable program from the perspective of good corporate governance. Might this not have been an effective device in all three of the corporate scandals referred to in the Introduction above? Clearly the risk to senior management of having compensation recaptured by their corporation when there is a restatement of income should result in more careful long-term planning. Principle No. 2 confirms senior management's role in enterprise risk management implementation, oversight and integration into company culture.

The scope of board fiduciary duty as to enterprise risk management appears to have broadened: With so much in the current management literature relating to the emergence and adoption of sophisticated ERM techniques, how can any board, collectively, be said to be acquitting its responsibility in this area, unless it specifically establishes internal procedures designed to inform itself of management action, enable it to evaluate such action over time and permit it to intervene effectively, based on adequate knowledge, so as to adopt appropriate corrective measures?

In this connection, we note there has been a proliferation of enterprise risk management approaches throughout the more professionally operated businesses that emphasize systematic risk analysis, including creation of cross-area reporting and use of committees to heighten awareness of interdependent risk elements, and periodic reporting within departments and up-stream to senior management. From the perspective of the board, accountability and continuity of focus are essential on issues ranging from counter-party risk, leverage and currency exposure, to product testing and/or the risks inherent in pursuing or implementing a merger or acquisition.

Responsibility for review and evaluation of every element of risk identification and pre-emption should be assigned in such a way as to encourage full and open discussion of vulnerabilities and potential risks and responses. The board member given this task should be trained in and experienced with risk management methodologies, including the structural aspects of risk monitoring and communication, and should present risk-amelioration as part of strategic planning for the enterprise at large, with a view to long-term results. He/she will, at the very least, assure that a risk management "command structure" is created within his/her company, that he/she receives regular reports from the senior manager charged with ERM implementation, and that he/she has access to the line personnel in risk management functions. The assignment of "portfolio responsibility" in this fashion, we would argue, is the best approach to assuring that the board fulfills its fiduciary duties within the mandates of good corporate governance.

Privately Held Companies

The board of the small private company, whether a new venture startup or a mature business with a successful operating history, has similar fiduciary responsibilities under corporate law to those imposed on directors of any NYSE or NASDAQ company. Further, the importance of deploying appropriate enterprise risk management techniques and having them inform strategic business planning is the same—although the scale and complexity of the ERM exercise will typically be much less. On the one hand, there may be no more than a few shareholders owning and operating the entity and constituting the board, so that board fiduciary responsibility is not a likely issue. The presence of a core group of founders/operators and a group of outside investors, however, would impose higher fiduciary duties on the board and impel serious consideration of ERM. Similarly, where there is complete family ownership, with several family members operating the business but a much larger number of relatively passive shareholders dependent on the others for leadership.

Good corporate governance principles are thus particularly relevant in the privately held company when outsider or non-controlling shareholders are a corporate constituency. Issues can arise out of asserted failings by the insiders to properly deploy ERM methodologies to protect the business for the long term benefit of all shareholders. Where board membership contains a majority elected by the insiders/operators, the pertinence of the good governance principles to the acquittal by the board of its fiduciary duties must be acknowledged.

Corporate good governance principles are particularly relevant in the **privately held company** when outsider or non-controlling shareholders are a corporate constituency.

In short, a private company board that fails to take appropriate ERM action may open itself up to liability in the same way as directors in publicly traded companies—though the claims may come from second or third-round start-up investors, or simply from cousin Mary's disaffected daughter, who has seen her hoped-for retirement evaporate.

Captive Insurance

The captive insurance company is a privately-owned insurance company, nowadays often organized by a corporate parent company or group of companies to provide coverage for retained risk. This coverage may be, for example, for a deductible under a policy issued by a commercial insurance company, or primary insurance which is re-insured with a commercial insurance company, or reinsurance provided to a commercial fronter or primary. The insurance captive may provide significant cost benefits over commercial insurance, arising out of group purchasing, retention of underwriting profit, reduction of administrative expense and careful tax planning. The captive may also offer the possibility of funding coverage simply not obtainable by the insured in the commercial market or otherwise prohibitively expensive. Captives are also being used in innovative ways to introduce and disseminate a high degree of enterprise risk management professionalism throughout both publicly traded and privately held entities.

Thus, the captive increasingly becomes the platform for addressing an organization's risks in a systematic way. It is, after all, providing insurance for various risks on an enterprise wide basis, and its personnel, if professionally trained in risk management and insurance disciplines, will be seen to possess large credibility within the organization. The insurance captive could be particularly well-situated to design and promote, for example, uniform risk-management procedures throughout the various components of the enterprise, to gain better knowledge, on a comparative basis, about what works in the particular business, and to provide better transparency, for the education of senior management in ERM principles.

In addition, since the insurance captive is part of the same group of corporate affiliates that includes the insureds, it is likely that responsibility for failure to implement an ERM program can be better pinpointed and, if need be, penalized. Insurance captives can provide continuity for ERM programs that include not only the traditional risks indicated earlier, but also emerging concerns such as cyber risk (identity theft, privacy invasion and account theft), as well as supply-chain disruption, drug contamination and counterfeiting. The insurance captive itself is subject to the good corporate governance principles at the level of its own board of directors and senior management, and also accountable at the level of its ultimate ownership.

Conclusion

We have seen how during recent years principles of good corporate governance and fiduciary responsibility have become interwoven with the adoption of more wide-ranging and "scientific" techniques for enterprise risk evaluation and amelioration. In addition, the acceptance by boards and management of the lessons gained from ERM methodologies to inform strategic planning has proceeded apace. It is likely that this process will continue as boards become more sophisticated in its application, and as responsibility for enterprise risk management policy is increasingly accepted by boards as a serious fiduciary duty. In a volatile market place, marked by events like those that befell Bear Stearns or AIG, corporations may be adding a new Senior Management position to those of CEO, CFO and CTO, namely, the "CRO," or Chief Risk Officer.