Executive Risks

A Boardroom Guide 2012/13

Published in association with Willis' FINEX Global division

Consulting Editor: Mark Wakefield
Executive Director, FINEX Global, Willis Limited

Published by White Page Ltd

whitepage

Contents

Executive Risks:
A Boardroom Guide 2012/13

6

Effective board oversight of risk management in the United States

Steven A Rosenblum,
Partner
Wachtell, Lipton,
Rosen & Katz

Corporate risk-taking and the monitoring of those risks have remained front and centre in the minds of boards of directors, legislators and the media, fixed there by the powerful mix of continuing worldwide financial instability, corporate crises, ever-increasing regulation, and anger and resentment at the alleged power of business and financial executives. The reputational damage to boards that fail to manage risk properly is a major threat, and Institutional Shareholder Services, the corporate governance and proxy adviser, now includes specific reference to risk oversight as part of its criteria for choosing when to recommend 'withhold' votes in director elections. This focus on the board's role has also led to increased public and governmental scrutiny of compensation arrangements and their relationship to risk taking.

Directors often ask about the proper role of the board in corporate risk management. As in other contexts, they cannot and should not be involved day to day but instead should assume a risk oversight role, satisfying themselves that the policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite. They should also ensure that these policies and procedures are functioning as directed, and that the necessary steps are taken to foster a culture of risk-aware decision making throughout the organisation. The board should establish that the chief executive and the senior executives are fully engaged in risk management, and should be aware of the type and magnitude of the company's principal risks.

In light of US disclosure requirements, the board should consider whether the company's compensation structure creates an incentive for excessive risk-taking. And it should send the message to the management and employees that comprehensive risk management is not an impediment to the conduct of business but is instead an integral part of the company's strategy, culture and business operations.

The risk oversight function of the board of directors

Tone at the top and corporate culture

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. But the assessment and mitigation of risk should be incorporated into all business decision making.

In setting the right 'tone at the top', 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 throughout the organisation and embedded in its strategy, with appropriate training for employees and regular compliance assessments.

Fiduciary duties

In the United States, the Delaware courts have developed the basic rule that directors are liable for a failure of board oversight only where there is a "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", and have noted that this is a "demanding test" (*In re Caremark International Inc Derivative Litigation*, 1996). Delaware Chancery Court decisions since *Caremark* have expanded upon that holding, while reaffirming its fundamental standard.

In the case *In re Citigroup Inc Shareholder Derivative Litigation* (2009), the Delaware Chancery Court dismissed claims that the defendant directors had breached their fiduciary duties by not properly monitoring and managing the business risks posed by sub-prime mortgage securities, and by ignoring alleged 'red flags' that consisted primarily of press reports and events indicating worsening conditions in the sub-prime and credit markets. The court reaffirmed the "extremely high burden" faced by plaintiffs in bringing a claim for personal director liability over a failure to monitor business risk, and said that a "sustained or systemic failure" to exercise oversight is needed to establish the lack of good faith that is a necessary condition for liability.

More recently, in *Goldman Sachs Group Inc Shareholder Litigation* (2011), the Delaware Chancery Court dismissed claims against directors of the bank based on allegations that they failed to properly oversee the company's alleged excessive risk-taking in sub-prime mortgage securities and caused reputational damage to the company by hedging risks in a manner that conflicted with the interests of its clients. The plaintiffs' allegations included the claim that Goldman Sachs' compensation structure, as overseen by the board of directors, gave management the incentive to make ever riskier investments, with any benefits going to management but with risks falling on the shareholders. In dismissing the plaintiffs' claims, the court said that in the absence of red flags, the manner in which a company evaluates the risks of a given business decision is protected by the Business Judgment Rule and will not be second-guessed by judges.

These cases set a high bar for showing a breach of fiduciary duty for failure to exercise oversight, and reaffirmed that boards are not required to undertake extraordinary efforts to uncover non-compliance within their companies, provided a monitoring system is in place. While directors may take some comfort from the protection afforded by these standards, they should also bear in mind that cases involving particularly egregious facts and circumstances and substantial shareholder losses could lead to a stricter standard.

Boards should adhere to reasonable and prudent practices and should not structure their risk management policies around the minimum requirements needed to satisfy the Business Judgment Rule. It should also be noted that courts have taken the view that if a breach of duty for failure to exercise oversight is found, directors will not be protected by corporate exculpation or indemnification provisions.

US federal laws and regulations

The US Dodd-Frank Act creates new risk management procedures principally for financial institutions. Dodd-Frank requires bank holding companies with total assets of US$10 billion or more, and certain other non-bank financial companies as well, to have a separate risk committee that includes at least one member with experience in managing risk for large organisations. While other companies are not required to have a separate risk committee, they may want to consider whether it might be useful or, alternatively, whether

they should expressly allocate risk oversight to other standing committees.

Under US securities laws and regulations, companies are required to disclose in their annual reports the extent of the board's role in risk oversight, such as how the function is administered, the effect it has on the board's process — for example, whether the people who oversee risk management report directly to the board as whole or to a committee such as the audit committee — and how risk is monitored. US companies are also required to discuss risk oversight in their proxy statements, including the extent to which risks arising from compensation policies are reasonably likely to have a "material adverse effect" on the company, and how its compensation policy, including for its non-executive officers, relates to risk management and risk-taking incentives.

Industry guidance

Various industry-specific regulators and private organisations publish suggested best practices for board oversight of risk management. Examples include reports by the National Association of Corporate Directors' Blue Ribbon Commission on Risk Governance, and the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The 2009 report from the National Association of Corporate Directors provided guidance and principles for risk oversight activities, including how to:

- understand the key drivers of success and risk in the company's strategy
- craft the right relationship between the board and its standing committees
- provide appropriate resources to support risk management systems
- monitor potential risks in the company's culture and incentive systems
- develop an effective risk dialogue with management.

In 2004, the COSO published an internationally recognised framework for managing enterprise risk. This presented eight interrelated components:

- the internal environment (tone of the organisation)
- setting objectives
- event identification
- risk assessment
- risk response
- control activities
- information and communications
- monitoring.

A further risk management release from the COSO in 2009 recommended specific steps for boards to take, such as understanding a company's risk philosophy, reviewing its portfolio against that appetite, and knowing the extent to which management has established an effective system of enterprise risk management.

In its 2010 progress report, the COSO recommended that the board focus, at least annually, on whether developments in a company's business or the overall business environment have "resulted in changes in the critical assumptions and inherent risks underlying the organization's strategy".

Recommendations for improving risk oversight

While a risk management system should be tailored to a specific company's requirements, in general it should:

- adequately identify the material risks faced by the company in a timely manner
- implement appropriate strategies that are responsive to the company's business strategies, specific risk exposures and risk tolerance thresholds
- integrate considerations of risk management into business decision making throughout the company
- transmit information on material risks to senior executives and, as appropriate, the board or relevant committees.

Specific measures that the board, management and relevant committees may consider as part of their risk management oversight include the following:

- reviewing the company's risk appetite and risk tolerance, the setting of aggregate and individual risk limits, the policies and procedures in place to hedge against risks, and the actions to be taken if risk limits are exceeded
- reviewing the categories of risk faced by the company, the likelihood of occurrence, the potential magnitude of those risks, and ways to mitigate them
- reviewing whether adequate procedures are in place to ensure that new or materially changed risks are properly and promptly identified, understood and accounted for in the actions of the company
- reviewing the respective risk oversight responsibilities of the board, management and committees, to ensure a shared understanding of accountabilities and roles
- reviewing the executive compensation structure to ensure it is creating proper incentives in light of the risks faced by the company
- reviewing the risk management policies adopted by management, including procedures for reporting matters to the board and committees, and assessing their effectiveness
- reviewing the steps taken by management to ensure adequate independence of the risk management function
- reviewing the processes for resolution of differences that might arise between risk management and business functions
- reviewing the qualifications and backgrounds of senior risk officers and the personnel policies applicable to risk management, to assess whether they are appropriate given the company's size and scope of operations
- reviewing how the risk management strategy is communicated to all appropriate groups within the company, and ensuring that internal communication channels exist that encourage the prompt and coherent flow of risk-related information across business units
- reviewing reports from management, independent auditors, internal auditors, legal counsel, regulators and outside experts, as appropriate, on the risks faced by the company.

In addition to these measures, the board may want to focus on identifying the external pressures that can push a company to take excessive risks. In particular, companies have come under increasing pressure from hedge funds and activist shareholders in recent years to produce short-term results, often at the expense of longer-term goals. These demands may include steps that would increase the company's risk profile, such as greater leverage to repurchase shares or pay out special dividends, or spin-offs that leave the resulting companies with smaller capitalisations. While such actions may make sense for some companies in some circumstances, the board should focus on the risk impact and be ready to resist measures that are not in the best interests of the company or its shareholders.

Locating the risk oversight function

Most US public company boards delegate primary oversight of risk management to the audit committee, while financial companies covered by the Dodd-Frank Act must have dedicated risk management committees. Whether a separate risk committee is the right approach for non-financial companies will depend on the industry and specific circumstances of the company. Boards should also bear in mind that different kinds of risk may be best suited to the expertise of different types of committee — rather than a single committee specialising in risk management. To date, separate risk committees remain uncommon outside the financial services industry.

If the primary oversight function is delegated to the company's audit committee, it should schedule time for periodic review of risk management outside its role in reviewing financial statements and accounting compliance. Risk issues may also

arise in the context of the work of other committees, even if they are not allocated a primary oversight function, and decision making in those committees should take into account the overall risk management system.

Lines of communication and information flow

The ability of the board or a committee to perform its oversight role depends, to a large extent, on the relationship and flow of information between the directors, senior management and the company's risk managers. If directors do not believe they are receiving sufficient information — on, for example, the external and internal risk environment, specific material exposures, risk response strategies, and the strengths and weaknesses of the overall system — they should be proactive in asking for more. Directors should work with management to agree on the type, format and frequency of risk information required by the board. High-quality, timely and credible information provides the foundation for effective responses.

Any committee charged with risk oversight should hold meetings with the executives primarily responsible for risk management, just as an audit committee meets regularly with the company's internal auditors and liaises with senior management. In addition, risk managers and senior executives should understand that they are empowered to inform the board of extraordinary risk issues outside the regular reporting procedures. In light of the *Caremark* standards discussed above, the board should feel comfortable that 'red flags' or 'yellow flags' are being reported.

Legal compliance programmes

Senior management should provide the board or committee with a review of the company's legal compliance programmes and how they are designed to address the company's risk profile and detect and prevent wrongdoing.

While these programmes will need to be tailored to the specific company's needs, there are a number of general principles to consider. As noted earlier, there should be a strong tone at the top, with the board and senior management emphasising that non-compliance will not be tolerated. The compliance programme should be designed by people with relevant expertise and will typically include interactive training as well as written materials. Compliance policies should be reviewed periodically in order to assess their effectiveness and to make any necessary changes. There should be consistency in enforcing stated policies through appropriate disciplinary measures. Finally, there should be clear reporting systems in place, both at employee and management levels, so that all staff understand when and to whom they should report suspected violations and so that management understands exactly what information the board or committee needs for its oversight purposes.

A company may choose to appoint a chief compliance officer and/or establish a compliance committee to administer the programme, including facilitating employee education and issuing periodic reminders. If a specific area of compliance is critical to the company's business, it may be worth developing a separate apparatus devoted to that area.

Anticipating future risks

Finally, an ongoing effort should be made to assess and analyse the most likely areas of future risk for the company, including how the patterns and interrelationships of existing risks may change and how the company's processes can adapt to them.

With good anticipation of future risks, a company can avoid or mitigate them before they escalate into crises. In reviewing risk management, the board or relevant committees should ask the executives to discuss the most likely sources of material future risks and how the company is addressing any potential vulnerability.