RISK MANAGEMENT: WHERE LIES THE BOARD?

Jerry Koh, Partner and Daniel Seow, Associate, Allen & Gledhill LLP

The 2008 financial crisis has led to greater pressure on companies to have in place sound systems of risk management and internal controls to identify, evaluate and manage risk. To this end, governments of leading economies have enacted legislation and measures to rein in risk liberality, with the US Dodd-Frank Wall Street Reform and Consumer Protection Act being but one example.

In Singapore, a number of non-statutory codes and guidelines shape the best practices landscape, the primary source of which is the Code of Corporate Governance (the "Code").

The Code and risk management

The Code operates on the premise that responsibility for ensuring appropriate corporate risk management lies with the board of directors, which has, under the Code, the responsibility of establishing a framework of prudent and effective controls that enables risks to be assessed and managed.

Notwithstanding the responsibility of risk management resting chiefly with the board, Principle 11 of the Code also provides clarity with regard to the role a company's management team is to adopt on the matter of corporate risk. The board should ensure that management maintains a sound system of risk management and internal controls to safeguard shareholders' interests and the company's assets, and should determine the nature and extent of the significant risks that the board is willing to take in achieving its strategic objectives.

Board-management relationship regarding risk management

The relationship between the board and management is reasonably clear. While the board need not be involved in the day-to-day management of risk, they should adopt a risk oversight role to satisfy itself that first, the risk management systems and procedures designed and implemented by management are consistent with the company's strategic objectives and risk appetite; second, these systems and procedures are functioning as intended; and third, adequate measures are being taken to inculcate a culture of risk-awareness and risk-adjusted decision-making throughout the organisation.

> "Under general law and the Singapore Companies Act, directors have a duty to exercise skill, care and diligence."

The general supervisory nature of the steps required of the board does not mean that the board has a heavily diluted risk management responsibility. Guideline 11.2 of the Code states that the board should, at least, annually review the adequacy and effectiveness of the company's risk management and internal control systems, including financial,

operational, compliance and information technology controls. Guideline 11.3 imposes annual report commentary requirements on the board. The recommendation of establishing a separate board risk committee to assist the Board in overseeing the company's risk management framework and policies (Guideline 11.4) further implies that the threshold for discharging the board's responsibilities under the Code is not low.

Another source of guidance for risk management is the non-statutory Risk Governance Guidance for Listed Boards (Risk Governance Guidance) issued by the Corporate Governance Council in 2012. It was published to provide practical guidance after the 2008 global financial crisis underscored the importance of companies taking an integrated, enterprise-wide perspective of their risk exposure. The Risk Governance Guidance is intended to be read alongside the Code and to afford more particularised content to Principle 11 of the Code.

The Risk Governance Guidance and risk management

The Risk Governance Guidance provides further detail in delineating the scope of the respective roles of the board and management. The board is to determine the company's risk policies and set directions that adequately address relevant risks by optimising risk-taking such that the company understands the risk-reward trade-off and makes a decision that is commensurate with its risk tolerance. The board should also periodically monitor the company's exposure to risk that could undermine its strategy, reputation or long-term viability. Further, the board has to ensure that management properly identifies risks relevant to the company and, where possible, put in place action plans to mitigate the risks identified, as well as provide oversight of management's risk management and internal control systems.

Correspondingly, the role of management includes the identification and management of such risks by designing, implementing and monitoring the risk management and internal control systems of the company in accordance with risk policies and directions from the board. The risk management and internal control systems should provide reasonable assurance for managing the company's risks, the safeguarding of its assets, the reliability of financial information, and compliance with laws and regulations.

On a more practical level, the following six factors should be considered in the board's deliberations in determining the company's risk management and internal control policies:

- The nature and extent of the risks facing the company;
- The extent and categories of risk that it regards as acceptable for the company to bear;
- The likelihood of the risks materialising;
- In respect of risks that do materialise, the company's ability to reduce the incidence and impact on its business;
- The risk-reward trade-off; and
- The adequacy of resources and availability of requisite experience to manage risks.

The Risk Governance Guidance also puts forth a recommended risk management process comprising five individual steps:

1. Establish context, the external context being the external business environment and the internal context being the intra-company culture and structure.
2. Identify risks, noting the difference between inherent risks (which are the risks that an event may occur assuming that no controls or risk treatment measures are implemented) and residual risks

(which are the risks that an event will occur after having taken into account any actual or proposed actions to mitigate it).

3. Analyse and evaluate risks to decide whether and which risks need to be treated and, for those that need to be treated, on the most appropriate risk treatment strategies and methods.
4. Treat the risks, with four main options: transfer the risk, avoid the risk, reduce the risk, or accept the risk.
5. Monitor and report the risks on a regular and periodic basis.

Legal position in singapore

Under general law and the Singapore Companies Act[1], directors have a duty to exercise skill, care and diligence. The duty to be skillful entails the requirement to have, at an objective minimum, a capability of understanding the company's affairs[2], while the duty to be diligent requires directors to be assiduous in the execution of their responsibilities. The standard of care and diligence expected of a director is objective, that is, whether he has exercised the same degree of care and diligence as a reasonable director found in his position[3]. Such a standard is circumstance-specific and depends on various factors such as the individual's role in the company, the type of decision being made, and the size and the business of the company[4].

A failure to institute the appropriate risk management processes may accordingly render a director in breach of the aforementioned duty to exercise skill, care and diligence. Nonetheless, the Singapore courts have exhibited judicial deference in interfering with commercial decisions taken by directors, and have articulated that judges should not, with the advantage of hindsight, substitute their own decisions in place of those made by directors in the honest and reasonable belief that they were in the best interests of the company[5]. It is therefore arguably the case that a director will be found in breach of his duties only where he has patently abdicated his risk management responsibilities.

Conclusion

While there has been no legislation or cases directly on the point of risk management in Singapore, the non-statutory codes and guidelines as well as related case law in Singapore are instructive in giving some form in this area regarding directors' duties. Case law in the other foreign jurisdictions such as the US and UK can provide a basis for comparison. Though a measure of judicial deference may be adopted by the Singapore courts, boards must nonetheless be careful to keep abreast of existing standards in the performance of their obligations, and discharge its risk management duties.

In this regard, it bears reiteration that the Code provides that boards will need to establish a structure of sound and effective risk control measures with an underlying level of acceptable risk decided upon. Boards are also expected to monitor the adequacy of the companies' risk management and internal control systems and to ensure adherence by management and other employees. ■

[1] See Section 157(1) of the Companies Act.

[2] See the Australian case of Commonwealth Bank of Australia v Friedrich (1991) 5 ACSR 115.

[3] See Daniels v Anderson (1995) 16 ACSR 607. The modern approach adopted in this case was affirmed by the Singapore High Court in Lim Weng Kee v PP [2002] 2 SLR(R) 848.

[4] See the Singapore case of Lim Weng Kee v PP [2002] 2 SLR(R) 848.

[5] See the Singapore case of ECRC Land Pte Ltd v Ho Wing On Christopher & Ors [2004] 1 SLR 105.