KPMG

Across the board

A newsletter for Malaysian directors

MALAYSIA

Issue 02/July 2006

How do Boards approach risk management?

Understanding the company's risk appetite through open communication between management and the Board

Risk Management is definitely not about completely eliminating risk, or not taking risks, which is strategic dead end. Rather, it's about intelligent risk taking to generate value and business confidence.

– Strategic Risk Management Survey (KPMG 2004)

In a dynamic market environment, the company's objectives, its internal organisation and the risks that the company face will continuously evolve.

Paragraph 11 of the *Statement on Internal Control: Guidance for Directors of Public Companies (ICG)*[1] makes reference to best practices of the Malaysian Code on Corporate Governance (the Code) which requires the board to fully understand both the principal risks the company face and its system of internal control, so that these risks can be identified, evaluated, managed and controlled. With this understanding, the board should be able to maintain a sound system of internal control to safeguard shareholders' investments and the company's assets.

What is risk management?

The following text from the *Australian/ New Zealand Standard 4360:2004*[2] provides a good definition of risk management:
"Risk management is the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects."

It is generally agreed that by definition, being in business is about taking risks. The critical point is understanding what the risks are, as it can be about probabilities, consequences and even opportunities. The board may have the tendency to overemphasise the downside of the proposal (risk) and neglect the potential opportunities (reward). Therefore, there is a need to strike a balance between risk and reward.

Cars have brakes so that they can go faster, not slower.

Boards are generally more sensitive towards financial risks, but often overlook other kinds of risk, including product risk and risks arising from economic developments, technological changes and regulatory decisions that can affect business models. The question is whether boards are fully involved in deliberating risks at a strategic level.

Contemporary risk management is seen as being excessively focused on compliance. This detailed compliance focus can be a risk itself as the board can unconsciously place undue reliance on that fact that everything has been 'complied' with, but this does not mean that things will not go wrong.

Therefore, risk management is not just about compliance but processes put in place by management to identify, evaluate

[1] Task Force on Internal Control, *Statement on Internal Control: Guidance for Directors of Public Listed Companies* (Bursa Malaysia, February 2001), p. 5.

and respond to potential risks that may impact the achievement of the organisation's objectives.

While boards are reasonably good at managing existing known risks, they may not be adept enough in anticipating emerging risks. Risk and its consequences feature more prominently now amid rapid technological changes and dissemination of information. Therefore, risk needs to be better linked to the strategic planning cycle, being continually updated and mapped against emerging trends and issues.

It is acknowledged that while some risks cannot be predicted, building a robust internal capacity to deal with the unexpected is an important aspect of risk management.

An appropriate risk framework (e.g. *COSO Enterprise Risk Management - Integrated Framework*[3] *or Australian/New Zealand Standard 4360:2004*[2]*)* and a methodical approach towards risk management is essential as it provides a common and consistent language on risk across an organisation. There is a need to bring the framework to life, ensuring that it will identify real risks and bring the likelihood and consequence perspectives of these risks to acceptable levels.

Risk culture

Organisational culture is a crucial factor in risk management. An appropriate attitude to risk has to permeate every level of the organisation. It is arguable whether the responsibility to set the risk culture lies with the management or the board.

A common view is that in a practical sense, the board does not 'set' the culture and that it is more a function of the CEO and other senior management. The board can only seek to find out and understand what the culture really is by asking questions. In addition, the board has to be prepared to make changes and express clear views if it finds the culture unacceptable, including making management changes.

Paragraph 22 of the ICG states that it is the role of management to implement board policies on risk and control. In fulfilling its responsibilities, management should identify and evaluate the risks faced by the company for consideration by the board and design, operate and monitor a suitable system of internal control which implements the policies adopted by the board.

It is important to close any gap between the board's and management's understanding of the organisation's risk appetite and tolerance. To reinforce the appropriate culture and behaviour, it is recommended for risk management-related key performance indicators (KPIs) to be included in individuals' performance assessments. These KPIs are usually derived from the risk review process.

Risk appetite and tolerance

Contemporary approaches to risk management call on the board to determine its appetite and tolerance for risk. If the board does not articulate and communicate its risk appetite and tolerance, the management will make assumptions about the matter, deciding for itself what is acceptable to the board. This can lead to an inappropriate filtering of information going to the board, excessive "spin" being put on proposals and opportunities being lost.

A gap in board and management perceptions of risk appetite can also have surprising consequences. Potential pitfalls occur when management misreads the board's risk appetite and tolerance, resutling in an imbalance between risk management considerations and desired business outcomes.

Defining risk appetite is not an easy task as there are no formulae for risk identification and tolerance setting, and that enunciating risk appetite can prove to be difficult in practice. Not all risks can be measured in a meaningful way or expressed in financial terms.

However, there may well be a need for distinction between general and specific risk appetites. A risk appetite can be defined in terms of specific proposals considered and decisions taken and the discussions around them. But expressing a risk appetite as a generality can be difficult. Some believed that risk appetite "bubbles up" from the risk review process.

Each board will deal with communicating its risk appetite and tolerance in a way that is appropriate for it. The use of a common framework across the organisation can assist, as does the over-arching culture. In any event, open discussion between the board and management is essential.

Structural issues

The nuts-and-bolts of board oversight of risk can bring out a range of views. For example, should board audit committees also embrace the risk management function, or should this be delegated to a separate committee?

For banking institutions under the supervision of Bank Negara Malaysia (BNM), the board of these institutions and their bank holding company is required to establish a Risk Management Committee (RMC) as one of the Board Committees, stipulated in Appendix 2 of BNM Guidelines GP 1: *Guidelines on Directorship in the Banking Institutions.*[4]

[2] Joint Technical Committee OB-007, *Risk Management* (Joint Australian/New Zealand Standard, 31 August 2004), p. 4.
[3] Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Enterprise Risk Management - Integrated Framework* (COSO, September 2004).
[4] *Guidelines on Corporate Governance for Licensed Institutions (Revised BNM/GP 1)* (Bank Negara Malaysia, September 2005

GP 1 states that the RMC is responsible for:

- reviewing and recommending risk management strategies, policies and risk tolerance for board's approval;
- reviewing and assessing adequacy of risk management policies and framework in identifying, measuring, monitoring and controlling risk and the extent to which these are operating effectively;
- ensuring that infrastructure, resources and systems are in place for risk management; and
- reviewing management's periodic reports on risk exposure, risk portfolio composition and risk management activities.

Apart from banking institutions and other financial institutions governed by BNM, the larger public listed companies in Malaysia have generally established a RMC headed by the CEO or a senior management member, reporting to an appropriate board committee (such as the Audit Committee or the Board RMC). The existence of a committee should not be seen as implying a fragmentation or diminution of responsibilities of the board as a whole.

It is recognised that for smaller companies and boards, the same efficiencies may not be apparent from a formal committee structure, especially if such a committee is composed of the same individuals.

Whatever structural approaches boards take to risk management, it is generally agreed that the distinction between strategic and operational risk is critical as it allows the board to prioritise its agenda and follow up on the key issues accordingly.

Though internal audit has a key role in monitoring risk management, this link does not always send the right message to the organisation, lacking the appropriate "cultural" feel, perhaps reflecting internal audit's traditional emphasis on compliance. Moving forward, the board should consider rooting for a risk-based internal audit.

In addition, the role of company secretary and legal counsel is gathering added importance in the current environment. Therefore, the role requires some refinement and the board needs to extract more value from observations and insights of the company secretary and legal counsel.

Reporting on risk

The board has a responsibility to enunciate and communicate the organisation's risk profile internally and externally. However, there can be practical problems in executing this task.

It is undeniable that risk disclosure is necessary to assist investors make more informed decisions.

Paragraph 40 of the ICG reinforces the need for listed companies to apply Principle DII in Part 1 of the Code, where the board should, as a minimum, disclose whether:

- there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company;
- the process has been in place for the year under review;
- the process is regularly reviewed by the board; and
- the process accords with the guidance in the ICG.

> "To know and not to do is really not to know."
>
> – Stephen R. Covey,
> Author of The 8th Habit

Conclusion

Being in business means that the company would continuously be exposed to risks and these risks are now emerging and evolving more quickly. The role of the board is to oversee the establishment and implementation of the risk management system, and to review the effectiveness of the company's implementation of that system. This requires the board to recognise possible risks faced by the company and its industry, and ensure that management is effective in managing risks as an integral part of good management.

The alternative to risk management is simply risky management - which brings about this pertinent question: Are the right things done with respect to risk management in your company today?

If you would like further information on any of the matters discussed in this publication, please talk to your usual contact at KPMG or contact the following partners of KPMG's Risk Advisory & Internal Audit Services practice:

I G Chandran
Tel. (603) 2095 3388, ext 2217
igc@kpmg.com.my

Lim Chee Hian
Tel. (603) 2095 3388, ext 8401
cheehianlim@kpmg.com.my

Lee Min On
Tel. (604) 227 2288
minonlee@kpmg.com.my

kpmg.com.my

More information

Audit Committee Institute (ACI) Malaysia is sponsored by KPMG in Malaysia and supported by the Institute of Internal Audit Malaysia (IIAM). The Institute's primary mission is to serve as a forum and dedicated resource to keep audit committees informed of regulatory matters, company law and accounting and auditing issues. Ultimately, the Institute seeks to enhance the committees' awareness of, commitment to, and ability to implement effective audit committee processes.

To learn more about Audit Committee Institute Malaysia or to access our resources, please visit our web site (www.kpmg.com.my/aci) or contact us by e–mail (aci@kpmg.com.my). You may also contact the following KPMG partners at the Audit Committee Institute Malaysia:

David Lim

Tel. (603) 2095 3388, ext 2002

davidlim@kpmg.com.my

Mohamed Raslan Abdul Rahman

Tel. (603) 2095 3388, ext 8003

mraslan@kpmg.com.my

Lim Chee Hian

Tel. (603) 2095 3388, ext 8401

cheehianlim@kpmg.com.my

We value your feedback

Please e–mail any comments you may have, including topics you would like to see in the future issues to aci@kpmg.com.my.

If you would like to be included in our mailing list, and/or if you prefer to receive *Across the board* via e–mail, please let us know simply by sending your contact details including e–mail address.