Taking The Right Risks

Risk Governance Defined

By Ng Siew Quan, Partner And
Alvin Chiang, Manager,
Risk & Control Solutions
PricewaterhouseCoopers LLP

It's All About Managing Risks

You may have realised that of late, the issue of dealing with risk and uncertainty has been a constant theme across many newspaper editorials worldwide. In particular, it is the inability to properly manage them that has led to sensational headlines being made.

It's never easy to navigate risks when you're the one in the driver's seat, but having sound fundamentals definitely helps.

Back To Basics

Recognising that good risk management goes hand-in-hand with good corporate governance, the Corporate Governance Council[1], in reviewing the Singapore Code of Corporate Governance, introduced the concept of Risk Governance as a key principle[2] to the Code.

The revised Code puts the mantle of Risk Governance squarely on the shoulders of the Board. To provide further clarity and guidance, the Council subsequently released a supplement titled "Risk Governance Guidance for Listed Boards".

Key information on risk governance is provided in the guidance, including the following areas:

- How the Board can carry out its responsibility of risk governance of the company
- Factors which the Board should collectively consider when overseeing the company's risk management framework and policies
- The Board's responsibilities in Risk Governance vis-à-vis Management's
- Emphasis is placed on the notion that risk governance cannot be approached from a "one-size-fits-all" angle, which is aligned with ISO 31000's principle[3] that risk management should be tailored to fit the organisation.

In essence, the document aims to provide Directors with guidance on

these salient questions[4]:

- What is Risk Governance?
- Who is responsible for Risk Governance and implementation of Risk Governance policies / measures?
- What constitutes a sound system of risk management and internal controls?
- What goes into a risk management policy?
- How can risk tolerance be determined?
- What does a risk management process look like?
- What are some of the key Information Technology ("IT") risks?
- How does the Board ensure that the risk management and internal controls system is adequate and effective?
- What should be disclosed in the company's annual report with respect to risk management and internal controls?

The Concept of Risk Governance

The guidance states that Risk Governance:

- Is the architecture within which risk management operates in a company
- Defines the way in which a company undertakes risk management
- Provides guidance for sound and informed decision-making and effective allocation of resources

Successful Risk Governance is therefore contingent on how effectively the Board and Management are able to work together in managing risks. Central to this is the Enterprise Risk Management (ERM) framework, which articulates and codifies how an organisation approaches and manages risk.

Defining Roles and Responsibilities

The guidance states that the role of the Board in the governance of risk is in providing oversight of the company's risk management and internal controls system.

Within the context of the company's business model and strategies, the Board

Recognising that good risk management goes hand-in-hand with good corporate governance, the Corporate Governance Council[1], in reviewing the Singapore Code of Corporate Governance, introduced the concept of Risk Governance as a key principle[2] to the Code.

> The revised Code puts the mantle of Risk Governance squarely on the shoulders of the Board. To provide further clarity and guidance, the Council subsequently released a supplement titled "Risk Governance Guidance for Listed Boards".

should work with Management in determining which risks to take, as well as how much of it. It should then ensure that Management has in place the necessary safeguards in place to manage those risks. The Board's oversight responsibility also includes reviewing the system periodically for adequacy and effectiveness.

If required, the Board may choose to establish a separate Board Committee to assist it. It could also consider including Risk Governance into the scope of the Audit Committee.

The role of Management lies primarily in the design and execution of the risk management and internal controls system in accordance with the risk policies and direction set by the Board. It is also responsible for providing the Board with the necessary information when it comes to the monitoring and reporting of risks.

To support the overall Enterprise Risk Management initiatives, the company may consider appointing a Chief Risk Officer to provide executive oversight and co-ordination.

Such a decision would depend on various factors, including the scale, diversity and complexity of the company's operations.

A Sound System Of Risk Management And Internal Controls

A sound system of risk management and internal controls contributes to the safeguarding of the company's assets and consequently shareholders' investment5. At the same time, one must also appreciate that it can only provide reasonable (but not absolute) assurance.

A thorough and regular evaluation of the nature and extent of risks to which the company is exposed can help contribute to the maintenance of a sound system of risk management and internal controls. This is where the Enterprise Risk Management (ERM) framework comes in.

Some principle ERM frameworks and standards listed in the guidance include:

- AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
- Committee of Sponsoring Organisations (COSO) Enterprise Risk Management – Integrated Framework
- ISO 31000:2009 Risk Management – Guidelines on Principles and Implementation of Risk Management

Conceptually, ERM frameworks should have in common the following six elements (as highlighted in the guidance):

- Risk Strategy and Policy: The consideration of risk as a company sets its strategic direction and policies
- Risk Process: How risk is identified, assessed and managed in day to day activities
- Risk Structure: The specific risk management functions and responsibilities established to sustain the focus on risk management
- Culture: The culture and behaviours that need to be developed and sustained to support effective risk management
- Risk Systems and Tools: The systems and tools used to facilitate the risk management process
- Assurance: How assurance is gained over the effective operation of the risk management framework

Simple But Not Simplistic

It's often said that that the devil lies in the details and same applies when it comes to rolling out an ERM framework. That's where the well-known adage "simplicity is the ultimate sophistication" comes in handy.

Operationalisation of the ERM framework is often cited as a key challenge by practitioners, and many failures in this aspect can be attributed to organisations committing the cardinal sin of over-designing the framework and processes such that no one understands how it works apart from the designer himself.

While excessive complexity is a no-no, the other extreme of must also be avoided. Over-simplification of risks for example, may result in the treatment of a symptom rather than the root cause.

Hence, the challenge is in developing an ERM framework that is simple enough

> The guidance states that the role of the Board in the governance of risk is in providing oversight of the company's risk management and internal controls system.

Table 1: The ERM Maturity Framework

Level of Maturity	Framework	Commitment	Ownership	Processes	Communication & Training	Measurement	HR Support	Oversight
Ad hoc	No Structured approach	Risk management Seems as unnecessary expense	No interest in using risk management	No tracking of Risk management	No formal risk management training	No risk assessment performed	No HR support	No standard reporting
Initial	Policy/process defined	Rules-based approach	Partially defined roles	Risk management champion drives implementation	Risk management material circulated	One-off requirements announced	New staff trained	Monitored by exception
Repeatable	Practical guidance provided	Proactive approach	Clearly defined roles	Managers drive implementation	Co-ordinated training provided	Repeat measurements reported	Risk management integrated into all training	Business units monitor own risks
Managed	Managers confirm compliance	Risk management embedded	Centre of excellence model	Business units drive implementation	Business units drive tailored training	Risks measured consistently	Risk management ability impacts hire/promote decisions	Single view of risk across organization
Excellence	Risk management central to decision making	Risk management used for strategic advantage	Managers pursue risk unconsciously	Board and CEO drive risk agenda	Training focuses on best practice	Risk-adjusted performance measures used	Risk management seamlessly integrated into HR	Business driven with key risk indicators

© 2012 PricewaterhouseCoopers LLP. Reproduced with permission.

> The role of Management lies primarily in the design and execution of the risk management and internal controls system in accordance with the risk policies and direction set by the Board. It is also responsible for providing the Board with the necessary information when it comes to the monitoring and reporting of risks.

for everyone to understand, yet robust enough to deal with complex risks. The best frameworks often are those that are simplest, both in design and execution. Risk management should not be "bolted on" your processes, but rather "built in".

Before embarking on an ERM programme, it would be useful to consider the current condition of your organisation's risk management framework and practices vis-à-vis your desired state. Our maturity framework in Table 1 provides a useful reference for this. The key to success lies in effective change management: understanding that the journey to excellence has to be progressive and cannot be rushed.

Connecting The dots: Linking Risk Management To The Business

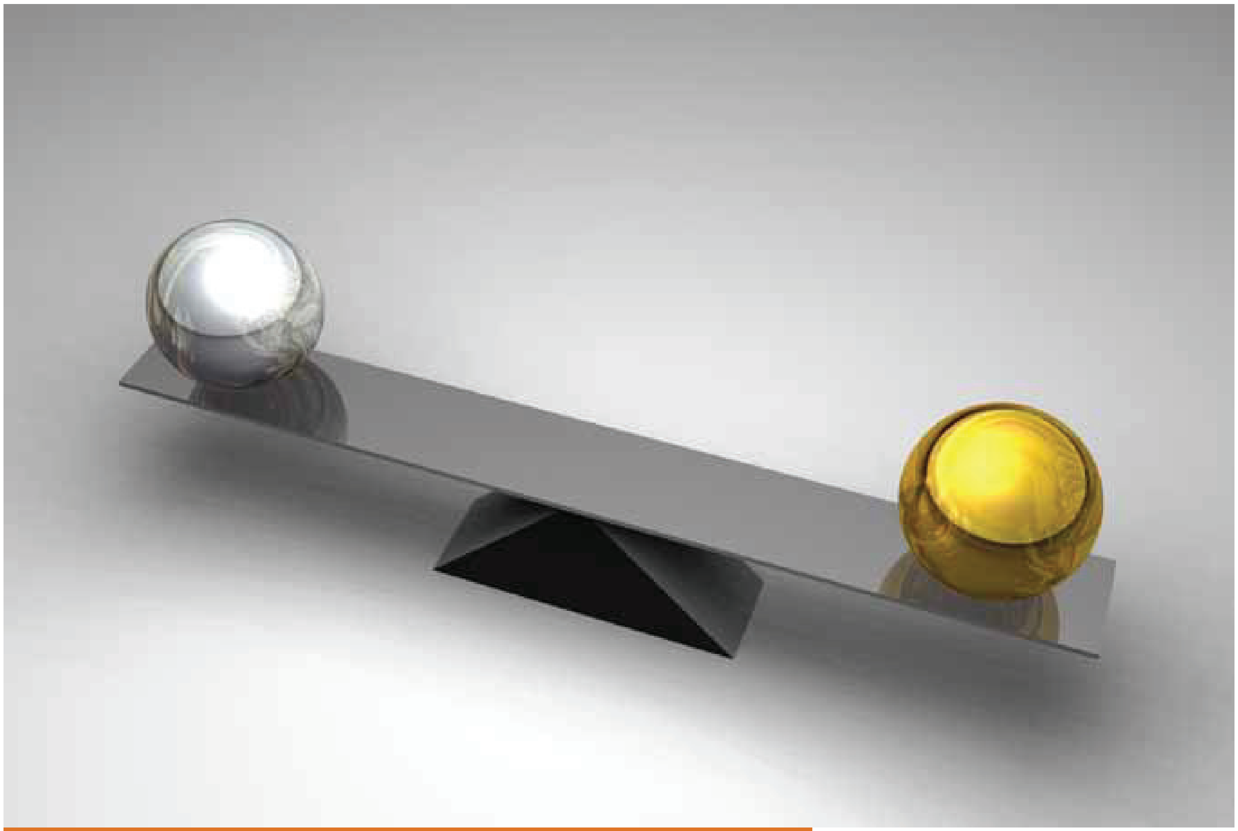
The other thing about risk management is that it should never be standalone, isolated from the other business processes. An effective risk management framework includes the necessary linkages to these processes and spells out the relationship between them.

For example, the articulation of business strategies should encompass the development of plans to address associated risks, which in turn should drive budget allocation. After all, there is little sense in having risk management plans without the necessary resources to execute them.

Ensuring An Adequate And Effective Risk Management And Internal Controls System

The Board should undertake an annual assessment for the purpose of making its public statement in the annual report on the adequacy and effectiveness of the company's risk management and internal control systems.

To ensure an adequate and effective risk management and internal controls system, the Board should first define the process to be adopted for its review of the risk management and internal controls system. It should then look into what significant risks have been identified and consider how effectively they are being managed. Is there a need for more monitoring and control for any particular risk? Are prompt actions taken to remedy significant failings or weaknesses in the risk management and internal control system?



The Board should undertake an annual assessment for the purpose of making its public statement in the annual report on the adequacy and effectiveness of the company's risk management and internal control systems.

What Goes Into The Annual Report

In providing a commentary in its annual report, the Board should summarise the process which it has applied in reviewing the adequacy and effectiveness of the system of risk management and internal controls. In addition, the Board should comment on whether the CEO and CFO have provided the Board with assurance on the integrity of the financial records / statements, as well the effectiveness of the company's risk management and internal control systems.

Taking Your Chances

Effective Risk Governance does not equate to being risk-adverse. As in the words of the poet T.S. Eliot:

"Only those who will risk going too far can possibly find out how far one can go."

It is therefore being smart about the risks you take, being adaptable to the constantly-changing business environment. It is about building resilience, ensuring that there are fail-safe mechanisms in place to cushion any unsuccessful gambits. These are the hallmarks of effective Risk Governance.

It is always useful to keep this in mind: the pursuit of any opportunity is always accompanied by an element of risk. How effectively we deal with these risks ultimately defines the extent of our success.

Endnotes:

1. The Corporate Governance Council was set up in February 2010 to review and update Singapore's Code of Corporate Governance

2. See Principle 11 of the Revised Code of Corporate Governance

3. ISO 31000:2009 Risk management — Principles and guidelines

4. Risk Governance Guidance for Listed Boards, Corporate Governance Council, 10 May 2012

5. Ibid.