Establishment of risk management committee

MCCG Intended Outcome 9.0

Companies make informed decisions about the level of risk they want to take and implement necessary controls to pursue their objectives.

The board is provided with reasonable assurance that adverse impact arising from a foreseeable future event or situation on the company's objectives is mitigated and managed.

MCCG Step Up 9.3
The board establishes a Risk Management Committee, which comprises a majority of independent directors, to oversee the company's risk management framework and policies.

The internalisation and application of the content "Why" and "How" should be read in tandem with the line of sight outlined by the Intended Outcome.

Why — The case for change

The marketplace is becoming increasingly complex as new waves of change are reshaping numerous industries, as illustrated in the diagram below:

Key changes in the current business context:

Source: On the 2017 board agenda, KPMG

What could go wrong:

- Inadequate attention and focus on risk management issues.
- Risks that do not fall neatly into the scope of a particular board committee may be overlooked.
- Undue reliance placed by the board on management and external experts for input on risk management.
- Deliberations on risk management are isolated from strategy and corporate culture.

The greater sophistication and complexity of businesses have significantly affected the way in which management implements key decisions. Being able to challenge management on how the company is responding to these signals and exposures necessitates greater attention at the oversight level.

Given the ongoing developments, it may be value-adding to institute a board committee to deal with the unique, complex, and volatile risks the company faces. A dedicated company-wide risk oversight by the board committee could go a long way in heightening scrutiny on risk management matters and thus enabling a more effective anticipation of, and reaction to, events and trends that could lead to disruptive changes in the business model. It also provides an opportunity to coordinate and monitor all key risk discussions in a transparent manner at a central point.

Point for reflection

A key driver for the establishment of a dedicated board risk management committee is the need for comprehensive views as opposed to silo perspectives.

At present, most of the committees and other governance mechanisms are **focused on one specific aspect of the company's risks**. For example, audit committees typically oversee financial reporting risks and certain compliance-related risks that can have financial reporting implications. Remuneration committees oversee risks related to how the remuneration structure drives behaviour within the company.

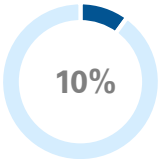
This oversight model commonly leaves other critical risks such as technological, litigation and environmental risks unattended, thus giving rise to the scenario dubbed as "**orphan risks syndrome**".

In the case of financial institutions, the need for a stand-alone risk management committee is even more compelling as **the nature of risks inherent in their operating models are varied and nuanced**. Exposures such as market, credit and liquidity risks are closely related to the fluctuating macroeconomic environment, thus rendering them volatile. These exposures elicit the deployment of complex risk infrastructures and call for greater scrutiny at the board level.

Recognising the significance of dedicated risk oversight in financial institutions, **Standard 12.1(c) of Bank Negara Malaysia's Policy Document on Corporate Governance** mandated the establishment of a risk management committee.

Investors' perspectives

The focus on risk management is a top governance priority of institutional investors. A 2016-2017 United States' National Association of Corporate Directors survey revealed that 10% or one in ten boards that met with institutional investors specifically discussed risk oversight.



This heightened scrutiny on risk management can also translate into shareholder campaigns and adverse voting recommendations. For example, in connection with the investigation on breaches of Foreign Corrupt Practices Act at a major multinational retail corporation during the year 2014, a proxy advisory firm, namely, the Institutional Shareholder Services ("ISS") recommended voting against the Chairman, Managing Director and Audit Committee Chair of the said retail corporation due to the board's failure to adequately communicate material risk factors to shareholders and assure shareholders that there is proper risk oversight in place[1].

[1] Lipton et. al 2017, *Risk Management and the Board of Directors,* Harvard Law School Forum on Corporate Governance and Financial Regulation

HOW The practice in substance

It is clear that whilst ultimate responsibility for a company's risk management framework rests with the board, having a risk management committee can be an efficient and effective mechanism to bring the transparency, focus and independent judgment needed to oversee the company's risk management framework.

Key considerations relating to the application of this Step Up are discussed below:

What are the key responsibilities of the risk management committee?

A risk management committee should have a charter that clearly sets out its role and provides it with all the necessary powers to perform that role. Some of the suggested responsibility areas that can be considered when outlining the terms of reference of a risk management committee are set out below:

Suggested risk oversight responsibilities (non-exhaustive)[2]:

- Determine that there is a robust process in place for identifying, managing, and monitoring critical risks; oversee execution of that process; and ensure it is continuously improved as the business environment changes.
- Provide timely input to management on critical risk issues.
- Engage management in an ongoing risk appetite dialogue as conditions and circumstances change and new opportunities arise.
- Oversee the conduct, and review the results, of company-wide risk assessments, including the identification and reporting of critical risks.
- Oversee the management of certain risks, with regard to the complexity and significance of these risk exposures.
- Provide advice to the board on risk strategies and coordinate the activities of the various standing board committees for risk oversight.
- Promote a healthy risk culture and watch for dysfunctional behaviour that could undermine the effectiveness of the risk management process (e.g. excessive risk-taking due to misaligned key performance indicators and remuneration schemes).

Care should be exercised to minimise overlaps in relation to specific risks that the risk committee is assigned to oversee (e.g. oversight of compliance risk by both the audit committee and risk management committee).

[2] *Board perspectives- risk oversight* 2015, Protiviti

Can a combined board committee lead to focused or dedicated oversight of risk management as envisaged by Step Up 9.3 of MCCG?

In determining whether there is dedicated oversight by the committee, the test would be the **balance of work performed by the committee and whether matters of risk are accorded with due attention**.

Under normal circumstances, a combined committee (e.g. audit and risk management committee) would not be considered as an application of **Step Up 9.3 of MCCG**. Combined committees are commonly overwhelmed with their primary agenda and may not have the expertise to oversee risk management matters in an effective manner.

What are the factors that should be taken into account in establishing the composition of a risk management committee?

In order to be able to discharge the committee's mandate effectively, a risk management committee should be of sufficient size and independence (majority independent directors) and its members between them should have a sufficient understanding of the industry in which the company operates. Having directors who have little knowledge of the industry or the business environment would not add value to the committee and its function, leading to substandard risk assessment.

Key factors in determining the committee's composition are outlined below:

Size

The risk management committee should be of an appropriate size (i.e. at least three members) so that members can deliberate in an effective manner and any changes to the composition can be managed without undue disruption.

Independence

The risk management committee should comprise a majority of independent directors to enable objective oversight of risk matters. Whilst executive directors have more in-depth knowledge on the exposures that the company is subjected to, it is widely held that executive directors have a greater propensity to take risks given that their evaluation and remuneration are usually linked to the company's performance.

Business/industry knowledge

Directors with risk management experience and strong industry or business knowledge can significantly add value to the deliberations of the risk committee, particularly on operational risks. Their knowledge on the subject matter relating to the industry and the external environment may help to provide a better understanding of business-specific issues or growing exposures.

Time commitment

The establishment of an additional committee demands the time of directors. As such, consideration should be given in appointing members who are able to devote the time and attention to the affairs of the risk management committee.

Dos

- ✓ Setting out the terms of reference which deals with the authority and duties and disclosing these terms on the company's website.
- ✓ Developing focused agenda items for the risk management committee and its reporting to the board.
- ✓ Establishing platforms for periodic engagement sessions between the risk management committee and senior management.

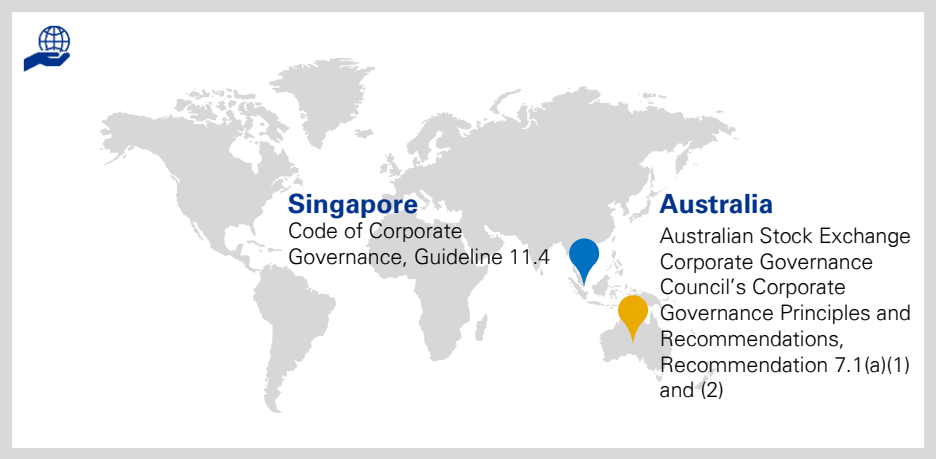
Don'ts

The following would render the application of this practice ineffective:

- × Having excessive overlaps in the responsibilities of a risk management committee and that of another board committee.

Where — Regional/international perspectives

Alongside Malaysia, selected jurisdictions including Australia and Singapore have also placed emphasis on the establishment of risk management committees in public listed companies premised on the evolving nature of risks in the corporate landscape which necessitates more focused oversight on risks.



Country	Provision
Australia	The board of a listed entity should have a committee or committees to oversee risk, each of which: (1) has at least three members, a majority of whom are independent directors; and (2) is chaired by an independent director. ***[Recommendation 7.1(a)(1) and (2)]***
Singapore	The Board may establish a separate board risk committee or otherwise assess appropriate means to assist it in carrying out its responsibility of overseeing the company's risk management framework and policies ***(Guideline 11.4)***.