

Risk Governance: Getting it right

By **IRVING LOW**
KPMG in Singapore

Boards are responsible for risk management and internal control, yet a study by the ISCA and KPMG shows that many continue to be challenged with handling this responsibility.

Managing risk is becoming more and more important as increasingly bizarre corporate debacles on wider scales have made eminently clear.

Increasingly, regulators and stakeholders are looking to the board and hanging responsibility on the board for a company's management of risk.

In Singapore, recent changes to the Singapore Exchange Listing Rules (1207 (10)) and Principle 11 of the revised Code of Corporate Governance 2012 (Code 2012) require boards to have more oversight of risk management and internal control.

Board accountabilities have increased as they must now disclose their views on the adequacy and effectiveness of risk management and internal control systems and provide an explanation as to how they have arrived at their conclusion.

As a result, SID's 2013 Board of Directors Survey (Ed Note: Check out *Aligning with the Revised Code* in Directors' Bulletin Quarter 1, 2014) identified risk management as the highest priority item on the agenda of most boards.

However, many boards are grappling with what their increased accountabilities mean in practice, revealed a recent joint study *Towards Better Risk*

Governance: A Study of Singapore Listed Companies 2013 conducted by KPMG in Singapore and the Institute of Singapore Chartered Accountants (ISCA). The study surveyed annual reports of a diverse group of 250 listed companies.

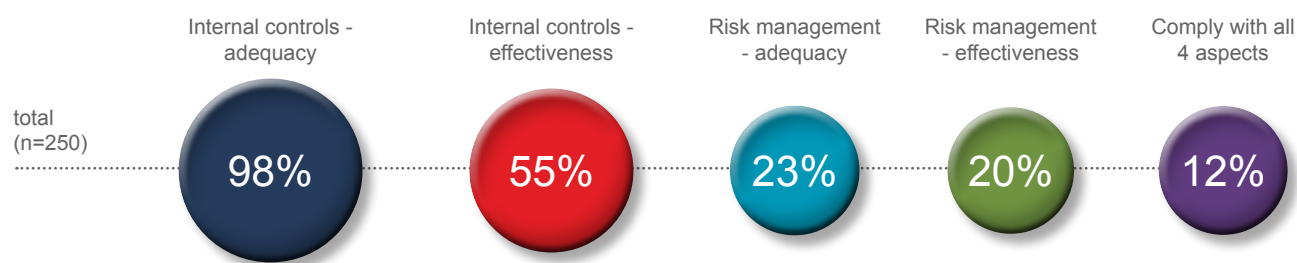
Companies are also challenged to determine and balance how much to communicate to stakeholders regarding their risk management and internal control systems.

Figure 1 shows the decline in compliance levels between mandatory and recommended requirements: 98% of the companies disclosed a board comment on the adequacy of internal controls as mandated by SGX Listing Rule 1207 (10). But only 12% disclosed a board statement on adequacy and effectiveness of risk management and internal controls, in accordance with recommended Guideline 11.3 of the Code 2012.

Results are surprisingly low as the concept of establishing robust risk management and internal control systems is not something new for Singapore listed companies.

The previous Code 2005 recommended that boards disclose the adequacy of internal controls and risk management. Yet the study

Figure 1: Whether the board commented or opined on the adequacy and effectiveness of the company's internal control and risk management systems



found that only 23% of companies adopted these requirements.

Who is Responsible

Principle 11 of the revised Code clearly states that boards are responsible for risk governance but may establish a Board Risk Committee, BRC, to assist. Yet, the ISCA-KPMG study found that 26% of respondents said responsibility lay with management while 22% did not state who was responsible. This highlights the need for organisations to clarify this fundamental requirement.

Stakeholders want assurance that risk governance accountabilities are clearly assigned within the organisation and the first step is to clarify what oversight structure is appropriate for their organisation, given the complexity of risks and scope of operations.

Boards typically delegate the oversight to the audit committee, although more organisations are establishing separate BRCs to enable more in-depth discussion on risks.

Regardless, boards must clearly articulate and document the terms of reference for the committees. Boards must also ensure these committees have the right composition in terms of skills and experience.

In addition, clearly defined reporting and communication structures must be set up

between committees and the board. Where risk is delegated to the audit committee, particular care must be taken to ensure there is sufficient time dedicated to fully understanding and reviewing the risk management and internal control systems.

Getting the Basics Right

The requirement to disclose more to stakeholders about risk management is a growing trend, yet the study found that only 32% of companies disclosed and explained their risk management framework in their annual reports.

As boards deal with the changing nature and velocity of risks (thanks to factors such as increased regulations, digitisation, globalisation and social media), having a defined and structured process to identify, measure, manage and monitor risks is critical to success.

In particular, boards need to ensure that:

- the organisation has set clear responsibilities for risk management at all levels through risk policies,
- decisions are made within agreed limits through risk tolerance,
- significant risks are understood in terms of what is currently in place to manage them and what else needs to be done to mitigate the risk to an acceptable level, and
- the organisation is responsive to change when unexpected events occur.

Most importantly, boards must set the right tone from the top to create an appropriate risk culture.

As boards increasingly demand improved risk information to assist their monitoring and oversight role, risk dashboards have emerged as a key tool to report risk information to boards. These dashboards capture salient risk/control/action information including Key Risk Indicators (KRIs) that align to risk tolerance levels and sources of assurance.

Confidence to Disclose

While the CEO and CFO are required to provide assurance to the board regarding the effectiveness of risk management and internal controls, the study showed that only 15% of the companies disclosed such an assurance (Refer to Figure 2).

This finding reflects possible difficulties that companies face in determining the extent of assurance required and what needs to be done to support the assurance.

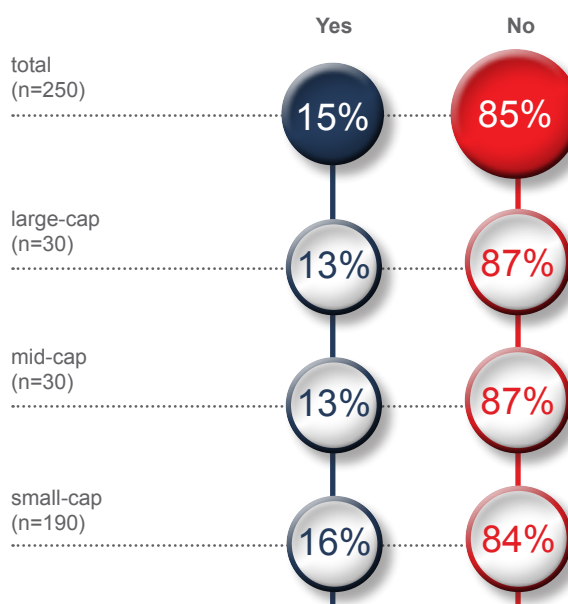
Boards, CEOs and CFOs can obtain assurance from a variety of sources: management, oversight functions such as Risk Management and/or Compliance, and/or independent assurance providers such as Internal Audit.

The study found that 94% of companies have some form of internal audit function in place, though only 39% of these met the Institute of Internal Auditors professional standards.

Another emerging area of assurance is the control self-assessment/certification programme. This is particularly important for large, complex organisations with thousands of employees and dozens of sub-business units, where it is very difficult for the CEO or CFO to ensure that every unit is operating properly.

The purposes of this programme are to raise awareness of risk and controls within and across

Figure 2: Did the company disclose that the CEO and CFO provided assurance?



the organisation and to enhance accountabilities for checking, monitoring and evidencing the adequacy and effectiveness of risk management and internal control systems.

Call to Action

The law is clear that the board is ultimately responsible. Directors, then, cannot be passive or merely reactive in risk management. Some immediate avenues that directors should consider include:

- Understand the board assurance framework for the organisation – this is a critical tool that connects the risk management, internal control and assurance system within and across organisations in relation to responsibilities, processes, reporting and communication channels.
- Review the positioning of the internal audit function to ensure it is focused on the right areas, is providing timely, accurate, insightful observations and that it provides directors with accurate and relevant information.

A take on risk

Boards should view risk management as good business practice, rather than a tick-the-box exercise in compliance.

“The question of how much to regulate is a tough one,” explained Accounting and Corporate Regulatory Authority Chief Executive Kenneth Yap at a forum and discussion hosted by KPMG and the Institute of Singapore Chartered Accountants (ISCA).

Mr Yap, one of five panelists, said: “We need to ask ourselves whether we want a system that is principles-based or one that is more prescriptive. The danger in being too prescriptive is that there is rarely one size that fits all. The other question is whether to mandate specific rules. Will this spur the desired behaviour? We have to be quite careful about forcing companies to fit into a specific set of check boxes as we might not get the desired results.”

SGX Chief Regulatory Officer Richard Teng concurred: “As a regulator, you don’t want to continually add new requirements as there are high costs related to introducing new rules. Instead, what we would like to do is

create an ecosystem that increases the rewards for companies that implement good risk governance.”

“Continually adding more rules and regulations can make it very onerous for companies. We have to be mindful of how to strike the right balance between control and governance versus freedom to pursue opportunities.”

The other panelists include Singapore Press Holdings CEO Alan Chan; Prof Ho Yew Kee, Head, Department of Accounting, NUS Business School; and SID Chairman Willie Cheng. The panel discussion was moderated by Irving Low, Partner and Head of Risk Consulting, KPMG in Singapore.

Prof Ho added that there needs to be a change in mindset so that companies view the implementation of sound risk management practices as a way to make their business stronger, rather than simply a regulatory obligation. “Regulation should not be the main driver of risk management, otherwise it can become a box-checking exercise. Companies need to get their house in order and proactively address risks.”

- Validate the adequacy and effectiveness of the control self-assessment programme to enable the CEO/CFO to provide meaningful assurances to the board.
- Seek external advice to validate management’s representations/disclosures regarding risk management and internal control. Principle 6.5 of Code 2012 states that the Board should have a procedure for directors to take independent professional advice at the company’s expense.

None can foretell the future and there will always be new black swan events. Yet companies governed by effective boards and are a step ahead of their competitors in adopting sound risk management and internal control practices, will be better placed to navigate the bumps in the road and ride out the storm should disaster strike. ■

Irving Low is the Head of Risk Consulting at KPMG in Singapore.