BEST PRACTICES IN ENTERPRISE RISK MANAGEMENT

Dennis Lee, Director, RSM Ethos Pte Ltd

It appears that many in the business management world still find enterprise risk management (ERM) a relatively new concept. However, its importance is often recognised even if it is not well implemented.

ERM importance

Findings from the *2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities* by the AICPA revealed that only 23 per cent of survey participants were of the view that their organisation's level of risk management was "mature" or "robust". In addition, 65 per cent reported that they were "somewhat" or "extensively" caught off guard by an operational surprise in the last five years. This shows that in today's complex and fast changing economic, geopolitical, technological, regulatory and competitive environment, developing and maintaining an adequate and effective risk management system has been and will continue to be a challenge for organisations.

In Singapore, the annual reports of most tier-one listed companies contain extensive disclosure of the risk management framework adopted as well as the various risks identified. However, the question remains whether these risk management frameworks can stand the test of time and help organisations weather "storms" unscathed and not get caught off-guard by operational surprises. In the recent global financial crisis, we have seen reports on huge financial losses, or even the collapse of organisations that had well-written risk management frameworks and detailed risk disclosures in their annual reports.

Since the introduction of SGX Listing Rule 1207(10) in 2011 requiring company boards to give an opinion on the adequacy of internal controls addressing financial, operational and compliance risks, there have been instances where company boards have given positive opinions, yet still encounter failures in governance or liquidity management a few short months later.

> "The question remains whether these … frameworks can stand the test of time"

What are the missing elements that could have prevented ineffective risk management? How should companies move beyond regulatory compliance to enjoy benefits of an effective risk management system?

An effective risk management process

An effective risk management framework should have five essential practices.

First, there should be greater board engagement in risk management. In the survey, *Asia Risk Report – The Top Concerns of Asia-Pacific Risk Managers*

published by *StrategicRISK* magazine, only 29 per cent of the participants reported that risk management is integrated into every board meeting of their respective organisations. In a recent corporate governance seminar, we found only 50 per cent of participants thought that the average board had a comprehensive understanding of the risks their company faced.

This shows the board needs to be more proactive in the governance of risk. Participants also indicated risk management and value protection as the number one advantage that independent directors bring to business owners. This underscores the importance of the roles independent directors play when advocating for time and effort to building a robust risk management process.

As a rule of thumb, risk management should address the risks that would impede the achievement of strategic objectives, which is why the board and management need to review and agree on key strategic objectives that align with the organisation's mission and vision. Without clearly defined strategic objectives, the board will not be able to set the appropriate risk appetite and risk tolerance limits for the company.

Secondly, there should be engagement and clear accountability of senior executives in managing risks.

In large organisations, there is a concern that risk management may be solely delegated to a separate function instead of coming under the ownership of senior operating executives. In smaller organisations, risk management may be seen as a compliance cost and a responsibility that can be fully transferred to an outsourced professional firm. These echo the findings of the AICPA Report, where 88 per cent of public listed boards see the need for increased senior executive involvement in risk oversight.

Best practices recommend that the responsibility for defining clear strategic objectives not stop at the corporate head office at the group level. All business units – divisions, subsidiaries, departments, etc. – should be involved in defining their own objectives. This forms the basis of setting risk appetite and risk tolerance limits for each business unit which can then be reviewed and approved by the Board Risk Committee.

What this means is that risk identification, assessment, rating and mitigation plans should be developed for each business unit. All heads of department should participate in cross-functional discussions concerning risk appetite, risk tolerance, risk identification, risk profiles and risk mitigation efforts. This promotes an open risk culture, coordination and mutual understanding or appreciation of risks, and elicits ideas from the management teams of the business units as a whole.

What follows is approved risk tolerances should be translated into and aligned with management's KPIs for performance management. This ensures that the right attitude and mindset is encouraged to deal with risk. The AICPA Report similarly showed that not enough progress has been made by listed companies to incorporate measures and outcomes relating to effective risk management in determining performance compensation.

Thirdly, the risk management function should be empowered and capabilities built. Where possible, it is advocated that the risk management function be independent of the operating management with a direct reporting line to the Board Risk Committee. Unfortunately, this structure has yet to be adopted by many organisations. The *2014 Asia Risk Report survey* revealed that only 28 per cent of senior risk executives were reporting directly to the Board or Board Committee. Similarly, the AICPA Report showed that only 32 per cent of Chief Risk Officers had the same direct reporting lines.

Best practices in enterprise risk management

The risk management function should be staffed by personnel with adequate business experience as well as knowledge of the company's businesses. It should facilitate and closely monitor the risk management process undertaken by operating management in defining key objectives, risk appetite, risk tolerance, risk identification, assessment, rating and mitigation.

Finally, the various lines of defences should be well coordinated. For effective internal control and risk management, the board must be served by the various lines of defence.

The *Three Lines of Defence in Effective Risk Management and Control* by the Institute of Internal Auditors articulate this concept well; that is, the lines of defence should not operate in silos and have to work hand in glove to be truly robust in managing enterprise risks.

Operational management are the ultimate risk owners and must establish controls and effectively execute risk management and control procedures as part of daily operations. It is necessary to embed and monitor the effectiveness of the procedure through Control Self-Assessment (CSA) frameworks and organisation-wide risk dashboards. It is also necessary to establish an effective incident management framework to review and develop action plans to address incidents and near misses.

Risk management, controllership and other compliance functions that are part of operational framework need to effectively monitor the operational management in executing the first line of defence.

Internal auditors need to review the adequacy and effectiveness of the risk management processes. Annual internal audit plans should be aligned with and focus on key enterprise risks.

The road is long

There is still a long journey ahead for any company to claim it is a truly risk resilient enterprise.

Boards and key executives need to take the right first steps, invest in a culture of "doing the right thing in the right way" and foster open and frank dialogues over challenges in effective risk oversight. There is nothing more dangerous than an illusionary and false sense of comfort from an under-performing risk management function. Those charged with oversight should revisit "risk management 101" and wholeheartedly question what value and benefits they expect from risk management. ■