Enterprise Risk Management – Issues and Challenges in the Malaysian Landscape March 2012

The global financial crisis which enveloped the world since 2007 and reaching its height in 2009, has critically repositioned the Board of Directors' responsibility for Enterprise Risk Management ("ERM"). Organizations have started to pay more attention to ERM, with best practices revolving around tackling of risks from a strategic perspective. More recently, Kweku Adoboli who cost UBS £1.3billion through fraud and false accounting, of which the Swiss bank was unaware due to weaknesses in their risk management and internal controls, has underscored heavily the importance of risk management in organizations during these turbulent times.

The *Internal Auditor* magazine by the IIA published an article in June 2007, "Moving Forward with ERM". It highlighted that some key roles of the Chief Risk Officer ("CRO") stated by the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management-Integrated Framework* were: champion the overall risk management function, drive the execution and integration of the process and as well as assist the Board of Directors in fulfilling their corporate governance responsibilities. The CRO should also assist the internal and external auditors in relying on ERM output for the purposes of auditing planning and execution.

The publication has also highlighted in late 2008, 12 implementation challenges of ERM and the role of internal auditors in the ERM implementation process. Among the challenges listed were the nurturing of a risk-aware culture within an organization, integrating strategy and employee KPIs into ERM implementation, selecting the right technology which is in line with its existing risk management framework, and at the very basic level, the accurate identification, assessment and evaluation of risks which flow from the organization's strategy. Besides the requirement of basic risk management training, internal auditors can contribute to the success and maturing of the whole initiative by educating the Board about ERM principles.

In Malaysia, the implementation of ERM has been receiving more attention in recent years. According to the Corporate Governance Blueprint 2011 by the Securities Commission of Malaysia, work has commenced to review the existing *Statement on Internal Control – Guidance for Directors of Public Listed Companies.* The objective of the review is to improve corporate disclosures on risk management systems and internal controls including addressing specific issues such as internal processes to highlight emergent risks to boards. A taskforce co-chaired by the Institute of Internal Auditors Malaysia (IIAM) and the Malaysian Institute of Accountants (MIA), comprising representatives from the SC, Bursa Malaysia, Companies Commission of Malaysia (CCM), professional bodies, industry organisations and audit firms, is undertaking this review.

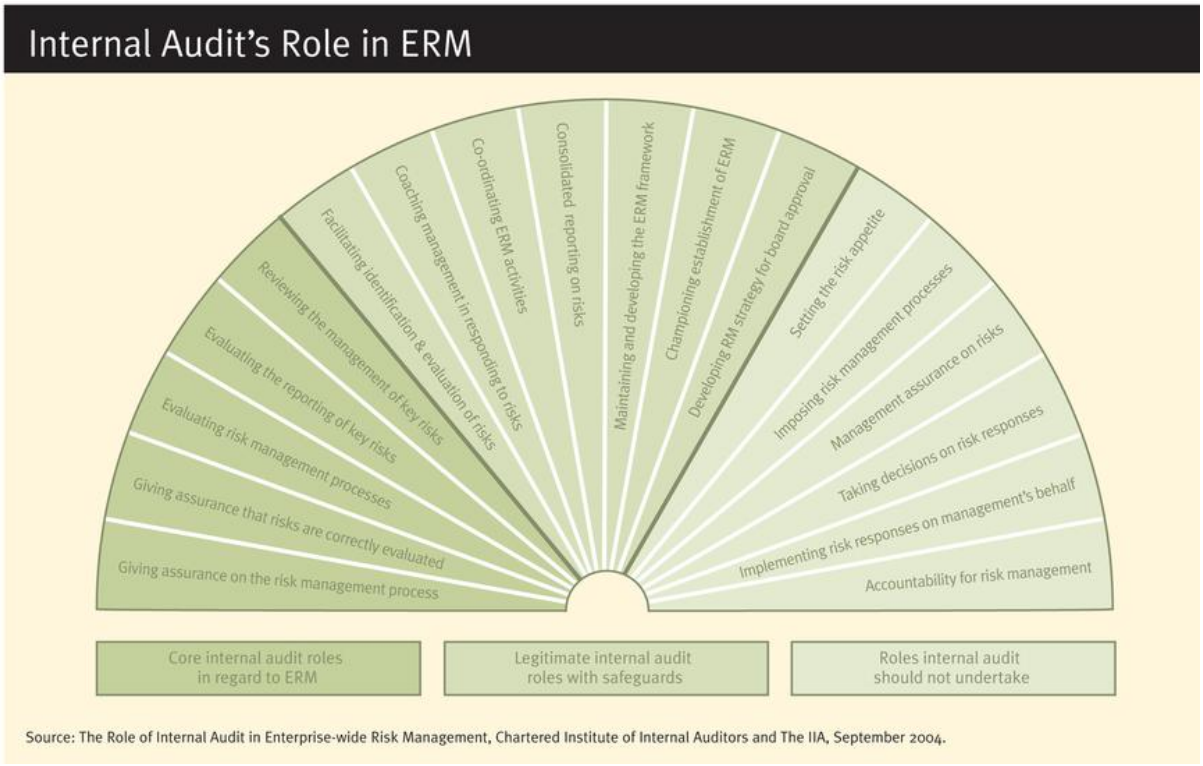
Research carried out among the main board listed companies on Bursa Malaysia (the Malaysian stock exchange) showed that ERM practices were still at an early stage in year 2008, whereby only 30% of the companies researched had in place some form of an ERM program. Further research was undertaken at the end of 2008 among 89 main board listed companies on Bursa Malaysia from the following seven industries: Technology, Industrial Products, Property, Consumer Products, Plantations, Trade and Services and Construction. ERM practices at that time were still at an early stage but appeared to be developing quickly. Approximately a third of them had already fully adopted ERM within their organizations.

From an Internal Audit perspective, the study showed that the quality of Internal Audit support very much affected the quality of the CRO and the openness of the Board of Directors towards the level of adoption of ERM in these companies. Therefore, the study concluded that Internal Audit support was crucial for the development of ERM practices in Malaysia. Subsequently in another local study, academics suggested that some of the obstacles to ERM implementation in these companies could be organizational structures which were not ERM-conducive, a general lack of subject matter understanding and difficulties in measuring risks.

A more recent study published in 2010 was conducted among 55 financial and non-financial public listed companies in the service sector on Bursa Malaysia. Results showed that the adoption and successful implementation of Enterprise-wide Risk Management was due not just to corporate governance compliance (Malaysian code of corporate governance and listing requirements) but also driven by internal factors such as good business practices, value creation, and survival. Companies in the financial sector were more focused on the internal risk reporting process and had risk management linked to the decision making process compared to the non-financial companies.

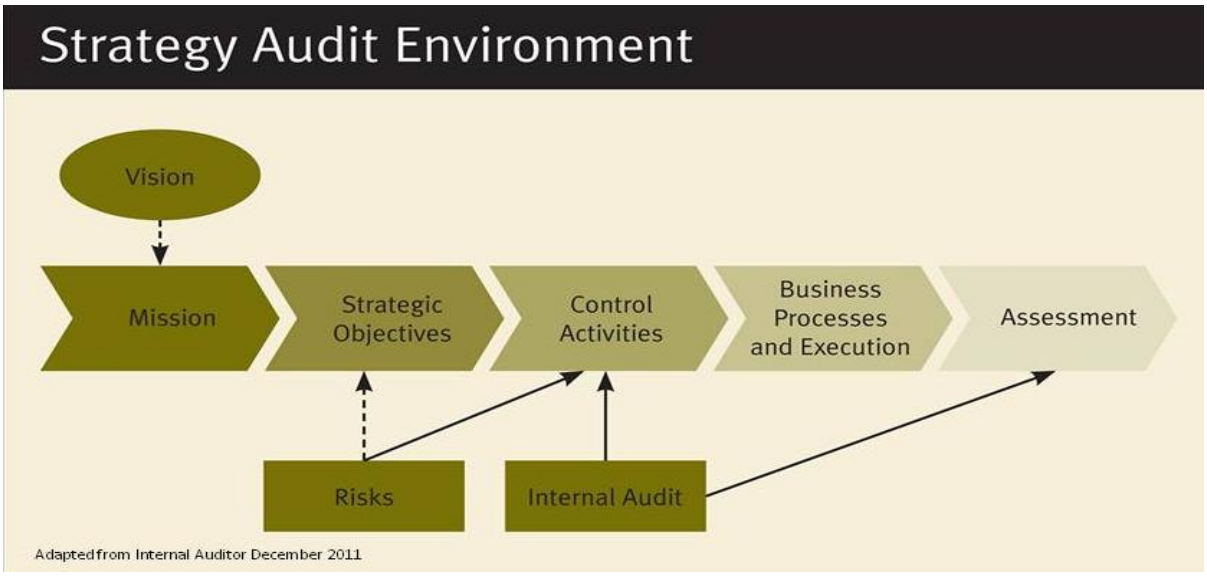
It is vital for the Malaysian Internal Audit profession to always bear in mind IIA's *International Professional Practices Framework* (*IPPF*) Performance *Standard 2120* on Risk Management which highlights that "the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." Furthermore, determining whether risk management processes are effective is a judgement resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.



The diagram above depicts the myriad roles that Internal Audit should or should not perform in the ERM process. At one end of the spectrum lie roles which are core in relation to the ERM function, such as giving assurance on and evaluating the risk management process, that risks are evaluated correctly and key risks are reported as well as managed. In the middle are roles which are legitimate such as facilitating the evaluation of risks, co-ordinating ERM activities or developing the risk management strategy for Board approval. However, Internal Auditors must be aware to not cross the fine line into activities which would compromise their independence such as taking risk response decisions, implementing risk responses on management's behalf and holding accountability for the risk management process.

It is also worthwhile for those in the Internal Audit profession to understand the relevance of ERM's role when Strategic Audits are performed. The Strategy Audit Environment (depicted below) establishes a clear link between the organization's vision, mission, strategic objectives, risks and subsequently the Internal Auditor's assessment of whether long-term strategy is on track or not.



As such, the CRO and Risk Management team plays a vital role in assisting business units with the accurate identification, evaluation and monitoring of risks (that arise from long-term strategic objectives), as well as control activities to address those risks. Internal Auditors then have the core responsibility of giving assurance to the Board on the whole risk management process. Another value-adding perspective would be also to evaluate how the organization addresses emerging risks and adopting a risk-based approach to governance reviews.

In practice, this structured process is still in its infancy where Malaysian companies are concerned. On the whole, risk management teams and business units still struggle with evaluating risks and proposing the appropriate control activities. Business units are seen to implement a quarterly review of risks and controls, with some companies weaving this process into their management KPIs.

In the wake of the global financial meltdown, the ISO 31000 was launched on 15 November 2009. As the new global standard for the implementation of risk management principles and guidelines, it applies to organizations regardless of size and sets out a process to manage risk in a transparent, systematic and credible manner. Four days later, it was presented in the Q-Radar Trail Blazer Alumni Conference, Kuala Lumpur. Conceptualized in 2004 by the ISO Meeting Group, it defines risk as the "effect of uncertainty on objectives". The standard addresses the entire management system and proposes a best-practice framework for risk management which involves every person in the organization from the board of directors down to the employees.

During the conference, the Chairman of the ISO Working Group which developed this standard and risk management expert Kevin Knight said that ISO 31000 was a more concise, clear and flexible set of guidelines developed for risk management. Before the ISO 31000, companies had adopted the AS/NZS 4360:2004 standard of risk management (Australia/New Zealand approach).

Kevin was quoted as saying, "It may take three to five years for bigger organisations to fully change their risk management standards as it will involve culture change in the organisation. We are talking about the complexity of certain big organisations here that may make it difficult for them to change their way of managing risk."

As such, it may be timely for more in-depth research to be conducted among Malaysian public-listed companies, young or old, on the extent to which ISO31000 has been adopted in their organizations and the maturity of their existing risk management functions.

A strong ERM function can effectively address the probability and consequences of risks. Addressing risks from a strategic perspective inevitably drives better strategic decision-making, heightens operational efficiency and enhances competitive advantage. In this respect, it is considerably important that the Board assumes the driver seat in ERM implementation and the CRO plays a key role in championing the process. However, every individual in the organization has a responsibility to manage risk according to a formal framework and should be trained in basic risk management skills.

The Corporate Governance Blueprint 2011 by the Securities Commission of Malaysia describes the Internal Auditor function as a traditional gatekeeper role, to provide independent and objective opinion as to whether risks which may hinder the company from achieving its objectives are being adequately evaluated, managed and controlled. Bearing this in mind, as well as IIA's recommendations and Malaysian research on the importance of Internal Auditors in the ERM process, Malaysia's Internal Auditors have a "unique opportunity and responsibility to identify emerging risks and support the board and risk teams as part of an effective, integrated governance, risk and assurance cycle" (Internal Auditor, Feb 2012). It would also be wise to increase their networking among risk management professionals in order to reposition themselves as expert advisors to the Board. Of paramount importance is the tone set by the Board at the top, which is always the key to driving successful ERM implementation in any organization.

CG Board Asia Pacific - Kuala Lumpur, Malaysia
For ERMA submission

References:

Yazid, A.S., Razali A.R. and Hussin, M.H. 2008. A Preliminary Study of Enterprise Risk Management Among Malaysian Business Enterprises. National Business Management Conference. Universiti Darul Iman Malaysia

International Review of Business Research Papers Vol. 5 No. 5 September 2009 Pp. 229-238, A Conceptual Framework For The Adoption of Enterprise Risk Management in Government-Linked Companies Wan Norhayate Wan Daud & Ahmad Shukri Yazid

The Role of the Quality Internal Adult Support in Enterprise Risk Management (ERM) Practices: Evidence from Malaysia. Wan Norhayate Wan Daud

International Review of Business Research Papers Volume 6. Number 2. July 2010 Pp. 239 - 252 239 Enterprise-Wide Risk Management (EWRM) Practices: Between Corporate Governance Compliance and Value Creation. Norlida Abdul Manab1, Isahak Kassim and Mohd Rasid Hussin

The Star: ISO 31000 will be more helpful in supporting corporate governance, Monday November 23, 2009

Schanfield, A. & D. Helming (2008). 12 ERM implementation challenges. Internal Auditor, 65(6), 41-44.

De La Rosa, S. Moving Forward with ERM. Internal Auditor, June 2007, pp. 50-54.

Baker, N. Extinguishing Emerging Risks. Internal Auditor, Feb 2012, pp. 32-37

Corporate Governance Blueprint 2011 by the Securities Commission of Malaysia

Malaysian Code of Corporate Governance (Revised 2007)