White Paper: The case for an enterprise-wide approach to risk management

Traditional Risk Management approaches within companies have mainly focused on operational risk. This has stemmed from the initial process where risk was related to the insurance industry with companies trying to secure the best liability cover for their potential risks at the lowest price possible (Waring & Glendon, 1998). This train of thought led to a fragmented risk management process within many companies, as individual business divisions assessed and prioritised the risks that were pertinent to their operations. This lack of inter-relationships and communication within a company's operations resulted on focus being placed primarily on physical and financial assets. Over time, companies began to realise, however, that the emphasis on loss prevention rather than adding value, was acting as a restraint in an ever increasing competitive and fast changing business environment.

In recognition for the requirement of an integrated and comprehensive strategic approach to managing risks, Enterprise Risk Management (ERM) has received increased attention in the Risk Management discipline and, in particular, within the corporate community over recent years. Although ERM is often substituted with terms such as holistic, strategic or integrated Risk Management, these adjectives generally refer to the same idea of managing all risks with the final objective of creating value. The Committee of Sponsoring Organisation of the Treadway Commission (COSO) provides a useful definition of ERM in their ERM - Integrated Framework Report (2004). It defines ERM is "a process effected by an entity's board of directors, management and other personnel, applied in strategy and across the enterprise, designed to identify potential events that may affect the entity... to provide reasonable assurance regarding the achievement of entity objectives".

Prior to providing the arguments that support the case for an enterprise-wide approach to risk management, it is necessary to firstly provide a brief overview of what ERM entails and how a company can go about creating and implementing a holistic risk management framework.

Overview of Enterprise Risk Management principle

The ERM approach differs from the traditional risk management approach as the focus is placed on an enterprise-wide strategy. Meilbroek (2002) argues that in order to achieve integrated risk management, a company must review and assess all the risks that could potentially affect its value. This core principle of ERM ensures that senior managers' focus is engaged on the uncertainties around the company's entire asset portfolio.

A second fundamental concept of ERM relates to the people that carry out and manage the process. Although ERM is the ultimate responsibility of the board of directors with the support of senior management, (i.e. a top-down process) it must be noted that in order for the approach to be enterprise-wide, every employee from every level of the organisation must support the framework. Without everyone's support into the process, the ERM infrastructure would be worthless.

Furthermore, as discussed in Protiviti's bulletin paper (2006), companies will need to be aware that they will require to be open and flexible to change. The ERM initiative can change organisational behaviour with the need for "building awareness, developing buy-in and ultimately driving the acceptance of ownership throughout the entity" (Protiviti's bulletin paper [2006]).

Enterprise Risk Management Framework

The COSO ERM framework (as described in the COSO Enterprise Risk Management - Integrated Framework report) provides a clear breakdown of the concepts and categories involved in the ERM process. The cube diagram is made up of four objectives (strategic, operations, reporting and compliance) eight components of ERM (objective setting, event identification, risk assessment, risk response, control activities, information & communication and monitoring) and

then finally the entity, its business units and divisions are described along the third dimension. According to the COSO report, this matrix enables senior management to focus on the company's complete ERM, or by component or unit. This 3-D diagram reflects the multidirectional process of the framework and illustrates that each component is reliant on another in order for the overall system to be effective.

Dickinson (2001) also provides a useful framework to define the process of enterprise risk. He suggests that enterprise risk begins with reviewing the corporate strategy objectives which may fail to meet the objectives of the enterprise. Various internal and external factors which can cause a company's activities to deviate from its corporate objectives, including changes in the economy, new competitors, systems failure, mistakes made by personnel etc, should be reviewed and assessed. By measuring the risks faced in line with the corporate objectives, a consistent framework is established (Dickinson, 2001).

Implementing Enterprise Risk Management

Once a company has decided to take the ERM approach, they will need to assess how to apply ERM to its corporate strategy. Knowledge Leader (enterprise risk management practical implementation ideas) recommends five simple steps for any company to follow which is considering implementing the ERM initiative. Firstly, the company should conduct an enterprise risk assessment to assess and prioritise the critical risks. Secondly, the company should define the risk management vision (through policies, procedures, reporting etc) and support it with ERM infrastructure. This could include the presence of risk management on the board, employing a Chief Risk Officer (CRO), establishing a risk committee etc. The next step would involve advancing the risk management capability of the organisation in one or two priority risk areas. Following this, a company should then re-evaluate the existing ERM infrastructure capability and develop strategy for advancing it. Finally the company should advance the risk management capabilities for key risks that were yet to be addressed in other areas within the company.

Drivers of Enterprise Risk Management

With ERM framework having been discussed, the background on how the requirement for ERM has arisen will now be addressed.

During the late 1980's and 1990's, the case for an enterprise-wide approach to risk management was heightened following the series of high profile business scandals and corporate governance failures. One of the most documented corporate failures was the events that led up to, and ultimately, the collapse of Barings Bank in 1995. Waring & Gledon (1998) suggests that the major financial losses and fraudulent activities, which resulted in the Barings Bank collapse, was a result of poor risk management.

The increased attention by the media and the government on company's activities, following these corporate failures, resulted in new corporate governance guidelines and legislation enforcing senior management to embrace wider corporate risk issues. For example within the UK, the publication the Cadbury, Hampel and Turnbull reports recommended guidelines on the maintenance of internal control within companies. This trend has progressed worldwide with various new regulations and procedures being introduced including the "Control and Transparency in Entities" law in Germany, Sarbanes-Oxley Act in the United States and the International Financial Standards.

The second reason for the rise in ERM over recent years, has come about from a "more general management thinking" (Dickinson, 2001). Contingency plans (plans, which identify potential threats and set out strategies in the event that the threats materialise) had been part of companys' policies for a long time. As indicated by Dickinson (2001), business continuation planning increased the practice of contingency planning by requiring more comprehensive internal systems. However both approaches were found to be limited as the strategic choices had already been made in the plans and the companies were limited to applying those plans.

How a company manages its risks depends on the choice of the corporate strategy the board wishes to take. For example, the board will need to decide whether to buy insurance or to hedge financial risks, whether operations and the risks that come with those activities, are best held within the company or transferred out. Over recent years, there has been a rise in companies utilising consultants to carry out certain activities. The oil and gas industry is in area where outsourcing is commonly used. By using an external individual that may be more knowledgeable and have a greater competence in a particular field, this can result in lower risk exposure (Dickinson, 2001). Waring & Glendon (1998) point out, however, that the drive towards "contract culture" is likely to have "an overall adverse effect on risks unless re-engineering is managed well".

Role of the CRO

With the increase in regulations and business risks, the appointments of CRO's have increased over the last few years and their influence within senior management and board of directors has strengthened. The very first CRO appointed can be traced back to August 1993 when GE Capital appointed James Lam to manage the combination of their credit, market and liquidity risk. As the business environment began to grow more complex during that time, Mr Lam's appointment had set the scene for the requirement of the CRO role in the business world.

The Economist Intelligence Unit's report (May 2005) which carried out a survey on 137 senior risk managers indicated that 45% of the companies, that had participated in their survey, had CRO already appointed as part of its senior management team. A further 24% were planning on filling the appointment over a two-year timescale. In addition, the survey indicates that the CRO plays a significant role within the company in enabling it to make positive strategic investment decisions and ensuring high standards of governance are maintained.

There are various benefits that companies can gain from having a CRO as part of the management team. The Economist Intelligence Unit's report (May 2005) survey asked participants what they thought was the greatest benefits of having a single manager with overall responsibility for risk. 52% stated that a CRO enabled the company to expand risk management to address more risks. 43% indicated that it enabled the business to make better investment decisions and 42% stated that a CRO assisted with enforcing better standards of governance. Further benefits listed included a reducing financial losses, reducing duplication in risk systems and processes, enabling the company to meet its compliance goals and deadlines, reducing the cost of risk management and increasing trust between the business and its shareholders and customers.

It is worth noting that an area that is posing a particular challenge to CRO's in today's business environment is digital risk. Digital risk can be defined, according to the Economic Intelligence Unit Report (2005), as the risks that are present from an increased dependency on information technology systems and digital processes. With companies facing more sophisticated IT systems and as well as new fraud and theft risks, IT risks can be amongst one of the most significant threats posed to companies' operations and one of the greatest challenges for CRO's to manage. The survey carried out in Economic Intelligence Unit Report (September 2005), which involved 218 senior managers, indicated that 48% of its senior risk managers respondents, believe that IT risk represents a high or very high threat on a company's operations. Nevertheless, IT risk can be managed by companies similar to how other risks are controlled, with senior management working together and applying an appropriate framework to assess the level of those risks faced . Egg Bank provides an example of this, with the CRO (who generally does not have a technology background) the Chief Information Officer (CIO) working closely together to overview the company's expenditure relating to IT risks (Digital Risk, Economist Intelligence Unit Report, September 2005). Bandyopadhyay et al (1999) proposed an integrated risk management framework which companies can apply to their IT systems. Believing that frameworks proposed in literature at that time had only incorporated some parts of IT risk management, Bandyopadhyay et al proposed a framework containing all four components of what they describe constructs the entire IT risk management system; risk identification, risk analysis, risk-reducing measures, and risk monitoring.

Advantages gained from Enterprise Risk Management

As discussed previously, although there are several benefits gained from a CRO managing a company's risk portfolio, there are further advantages a company can obtain from the overall enterprise-wide risk management system. By reviewing all potential risks that a company may be faced with, managers will gain an improved understanding of financial and operating risks and new insights on the interconnectivity between various risks and financial decisions. As indicated by Meulbroek (2002), this insight will reduce the total risk a company can face, it can protect and enhance a firm's reputation and reduce the likelihood of suffering from financial distress. Meulbroek (2002) provides Microsoft Corporation as an example of what could occur to an established successful company if it did not identify and assess all risks that can affect its value. If Microsoft was to be faced with an event that threatened the company's capability, it could witness, amongst several effects, a dramatic drop in customer numbers that could destroy the company's value.

The ERM strategy can also reduce costs spent on risks by eliminating duplication and increase administrative efficiencies across lines of business. An integrated approach enables companies to maintain competitive advantage. Fierce competition, rapid innovations, new standards and regulations etc can all affect a company's strategy. Nevertheless, by having a greater understanding on the company's entire risk portfolio through ERM, the company can respond quickly when faced with a changing environment.

A well-known example of a successful ERM implemented program was with space avionics company, Honeywell in 1997 (Banks 2004). The company spent two years of intensive planning on the ERM program with the assistance of the insurance broker, Marsh, the accountancy firm Deloitte & Touche and the insurer AIG. Prior to the ERM program, Honeywell (with over 50,000 employees in 95 countries) had a fragmented and decentralised risk management policy. The company's treasury group had two departments which as responsible for the financial and insurance risks. Insurance risks were covered by various annual policies and the majority of the company's financial risk management focus was placed on currency exposure (Banks, 2004). The ERM program aimed to reduce the company's risk costs by bringing together all of the various insurance risks into one single policy with a single multi-year cover of insurance risks and currency translation risks underwritten by AIG. Simulation techniques were introduced to estimate expected losses and communication was improved with scheduled joint meetings. The effect of the program was estimated annual savings (through reduced risk costs) of 15 to 20% and an overall reduction in the company's cost of risks from $38.7 million to $34.6 million (Banks 2004). Although Honeywell's ERM program eventually disintegrated with its take over by Allied Signal, this case study provided a positive example for other companies at that time.

Challenges in implementing Enterprise Risk Management

Although ERM has its success stories, one must note that it can be quite a challenge for company to implement such a successful enterprise-wide approach to risk management and that there are limitations that exist with such an approach. Companies must keep in mind that ERM is an approach that takes time to develop and implement and will not happen overnight. As each company faces different categories of risk, so too will they need different approaches to ERM to ensure the risks are covered and the tools used to address that risk is appropriate.

Change, as previously discussed, is also a fundamental principle of ERM which companies must be open and flexible too. Furthermore, in order for ERM to be successful, everyone must buy into the process. If not, then a breakdown in the approach will occur resulting in a less effective holistic risk management strategy. This also applies to a number of external parties. As indicated by Waring & Glendon (1998), different risk professions value their separateness and may fear that integration of ideas will lead to professional power struggles to control an integrated function.

Many empirical studies carried out over the years have confirmed that human judgement in decision making can be biased and flawed. Therefore management judgements and potential decisions on issues relating to risks, costs, benefits etc can lead to errors and mistakes, which in turn, could result in further exposure to new risks.

Conclusion

In summary, the goal of enterprise-wide approach to risk management is for all possible risks to be covered based on a portfolio view. The approach requires a consistent enterprise wide process, policies and systems integrating internal and external reporting. This process can be supported by having a CRO to implement and report on these processes to the management team. Staff will require to be continuously educated and trained so that everyone understands their role and contribution to the company's strategy. The quality management system and culture within the company will also contribute to the success of ERM, as staff will understand the importance of learning from previous experiences and to be able to act on decisions when needed.

As emphasised as part by Mundy (2001), the overall aim of ERM is to "restore a sense of perspective to the entire management process". This sense of perspective can help companies achieve their strategic goals. By understanding the risks involved, managers will have the confidence to seek out new business opportunities and encourage the business to grow and compete successfully within a fierce market place.

Bibliography:

- Badyopadhyay, K., Mykytyn, P., P., and Mykytyn, K. (1999*).* A framework for integrated risk management in information technology*, Management Decision*, Vol 37 (5), pp.437-445
- Banks, E. 2004. *Alternative risk transfer: Integrated Risk Management through Insurance, Reinsurance and the Capital Markets*, John Wiley & Sons Ltd
- Barton, Thomas, L., 2002. *Making enterprise risk management pay off,* Financial Times/Prentice Hall.
- Cadbury, A. 2002. *Corporate Governance and Chairmanship - A personal view*, Oxford University Press, Oxford.
- Coyle, B. 2002.*Risk Awareness and Corporate Governance*, Financial World Publishing
- Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation, *The Geneva Papers on Risk and Insurance*, Vol 26 (3), pp.360-366
- Galloway D., and Funston R. *The Challenges of enterprise risk management*, Balance Sheet, Vol 8 (6) pp22-25.
- Hopkin, P. 2002. *Holistic Risk Management In Practice*, Witherby Publishers
- Meulbroek, L. (2002). The Promise and Challenge of Integrated Risk Management, *Risk Management and Insurance Review,* Vol 5 (1), pp55-66
- Mundy, C. (2001). Enterprise risk: who knows my business better than me? *Balance Sheet*, Vol 9 (2) pp.12-15
- Reuvid, J. 2005. *Managing Business Risk*, Kogan Page Ltd
- Waring A, and Glendon A.I. 1998. Managing Risk, Thomson
- Young, P.C. (2001). Enterprise Risk Management: Another Perspective*,* Risk and Insurance Review, July 2001.

Online reference:

- Knowledge Leader :

http://www.knowledgeleader.com/KnowledgeLeader/Content:

- Enterprise Risk Management - integrated Framework: Executive Summary. September 2004.
- Enterprise business risk management process -overview
- Enterprise Risk Management and Risk Assessment Resources
- Enterprise Risk Management - Practical Implementation Ideas
- (COSO) Enterprise Risk Managment - Integrated Framework, Executive Summary, September 2004
- Enterprise Risk Management, Practical Implementation Advice, The Bulletin, Volume 2, Issue 6

- Economist Intelligence Unit Reports:
http://www.aceeuropeangroup.com/AceEuropeRoot/Media+Centre/Research/EIU+Survey

- The evolving role of the CRO, May 2005
- Digital Risk, the challenge for the CRO, September 2005

- Risk Management Reports:

www.riskmanagementreports.com

- Enterprise Risk Management: Past, Present and Future, May 2003, Vol 30 (5)
- Fresh views on Enterprise Risk Management, February 2007, Vol 34, (2)

Janice Flanagan is a Senior Consultant in Turner & Townsend's Management Consultancy services division, based in our Edinburgh office. She is also part of the Performance Improvement team. She has an MSc in Risk Management and wrote this paper while gaining her qualification.