Chapter 2

Literature review

2.0 Introduction

This chapter deals with the survey of existing literature in greater depth in the areas of risk based auditing and the internal auditor's adoption of the risk based approach to auditing. This section also extends to cover literature on the evolution of internal auditing practice as well as the extent of internal auditing's involvements in ERM. Salient findings from related research studies carried out in this area will also be discussed.

Following the financial scandals in the 1980s, the internal audit function, has become a domain of interest for academics, business practitioners and consultants (M. Allegrini et. al, 2009). There have been recent studies conducted to investigate the internal auditing practices at organisation level (Abdolmohammadi, 2009; Melville, 2003; Selim et al., 2003, 2009). Evidences were found that internal auditing practices also related to internal control and risk management practices (Selim and McNamee, 1999; Allegrini and D'Onza, 2003). The study conducted by Castanheira, Rodrigues & Craig (2009) on the Portugese companies, investigates the association of company-specific factors with the adoption of risk-based auditing as well as explores the role of internal auditing in enterprise risk management (ERM). This paper shall extend the study in greater depth in the Malaysia corporate environment.

2.1 Risk Based Approach to Internal Auditing

In early twenty-first century, the evolutionary practice of internal auditing resulted in the development of internal audit best practices which shifted the IA's focus from systems-based auditing to process-based auditing to risk-based auditing (IIA – UK and Ireland, 2003). The enactment of Sarbanes-Oxley Act of 2002 (SOX) in US has forced the management to establish objectives, identifying risks that affect those objectives and coming up with control measures to mitigate those risks although the focus is primarily only on internal controls over financial statements and disclosures. SOX mandated organisations to assess control against a suitable internal control framework (Matyjewicz and D'Arcangelo, 2004).

In planning and executing audit tasks, internal auditors would consider the approproate audit approach based on the effectiveness and efficiency of the approach in accomplishing the task at hand. There are generally three types of audits which internal auditors perform and they are compliance, operational, and financial audits. The objective of these audit types is to support the auditee's assertions. In a compliance audit, the auditee provides assurance that it is in compliance with the applicable laws, rules, regulations, and policies whilst in operational audits, the auditee's assertions relate to the efficiency and effectiveness of operations. The auditee, in the process performance of financial statement audit, would provide assurance that the financial statements are fairly presented (Colbert and Alderman, 1995). A risk-driven approach on the other hand, involves assessing, during the annual audit planning stage, the risks inherent in each audit area. Specific audit procedures would only be established after considering the risks involved. The goal of the audit planning process is to customised a dynamic, risk based and defensible audit plan that addresses all the needs of the

organisation (Verschoor, 2006). The fact that risk-driven approach helps internal auditors to focus their efforts on areas which are relatively more risky, it is hence regarded as more effective in meeting the objectives, and also efficient as it focuses on areas which are riskier as compared to the procedures-driven approach (Colbert & Alderman, 1995). By identifying, assessing, and monitoring a company's risk, internal auditing helps to ensure that adequate resources are deployed and focused on priorities (Kunkel, 2004). In short, risk based auditing focuses on assessing the goals, risks and controls that are infused in the organization's success (Rivenbark, 2000). While risk assessment is an essential part of the audit planning process, internal audit departments are finding their resources are limited with the scope of audit and the associated risk exposures ever increasing in the challenging environment (Kanter et al., 1990). By adopting a risk-driven approach where the audit engagement objectives, auditee's assertions and risks are considered, the internal auditor can assure that appropriate focus and resources are given to risky areas and that audits can be performed in the most efficient and effective manner (Alderman & Tabor, 1989). In this respect, the risk based approach to auditing allows more effective planning, execution and communication in order to better align the results to achieve the audit objectives set.

At the individual audit unit level in a risk based model, auditing procedures should be designed to achieve the objective that the controls in place are adequate. The internal auditor should understand the control and its environment; evaluating the adequacy of controls and test these controls are functioning as designed and effective (Walz, 1991).

In a survey conducted by Allegrini and D'Onza (2003), 25 % of the top 100 listed companies in Italy performed traditional compliance activities and generally adopted an audit cycle approach to planning for their annual audit schedule. About two third of the respondents adopted the risk-based approach for their annual audit planning whilst a few large companies adopted risk-based approaches at their annual audit planning as well as for individual audit assignments. In another study commissioned by IIA – UK and Ireland together with KPMG in 2005, it was found that some 89% of the respondents use a risk based approach in planning their annual internal audit plan whilst 93% were found to be adopting a risk based method in their individual internal audit assignments. This study also revealed a good 32% of the respondents are responsible for both compliance or risk management activities.

Table 2.1 below which is extracted from "Risk Management: Changing the Internal Auditor's Paradigm (McNamee and Selim, 1998)" aptly differentiates the risk based approach which widely regarded as 'best practice' from the Control based approach which is also commonly used by IA in their auditing work:

Characteristic	Control Based	Risk Based
Internal audit focus	Internal control	Business risk
Internal audit response	Reactive, after-the-fact, discontinuos, observers of strategic planning initiatives	Co-active, real-time, continuous monitoring, participants in strategic planning
Risk Assessment	Risk factors	Scenario planning
Internal audit tests	Important controls	Important risks
Internal audit method	Emphasis on the completeness of detail controls testing	Emphasis on the significance of broad business risks covered
Internal audit recommendations	Internal audit • Strengthened • Cost-benefit • Efficient/effective	Risk management • Avoid/diversity risk • Share/transfer risk • Control/accept risk
Internal audit reports	Addressing the functional controls	Addressing the process risks
Internal audit role in organisation	Independent appraisal function	Integrated risk management and corporate in governance

Table 2.1 Changing the Internal Auditor's Paradigm

Castanheira, Rodrigues and Craig, R., (2009), in their study on Portugese companies identified 5 factors that influence the adoption of risk based auditing approach and they are i) size of the organisation; ii) the industry which the organisation is in; iii) the sector ie. public or private sector within which the organisation belongs; iv) the extent of internationalisation of the organisation and v) listing status as the main factors that associated with the adoption of risk based auditing. This survey had also produced some interesting findings. Listed companies and those with extensive international presence were found to have a signification association to the adoption of risk based approach in annual audit planning whilst private, large and those companies in the finance sector were found to have strong but not significant association in this respect. When it comes to planning individual audit assignment, the risk based approach

correlates positively with the size of the organisation. These findings to a large extent shed light on the Internal Auditors' decision to adopt the risk based approach in planning their annual audit work (at macro level) as well as executing their individual audit assignments.

2.2 Internal Auditing Function

Traditionally, internal auditors have focused on financial reporting related internal control. Staciokas and Rupsys (2005) however assert that despite the different functions of internal auditing, the objective of internal auditing function is essentially to improve the entity's operations. However, the scope and function of internal audit have increased in response to changes in the business environment over the decades, shifting the focus of their audit work from financial statement and accounting functions to compliance audit, assessing the internal control and operating processes, and in recent years, adding risk management to their existing role. The internal auditing function has evolved along with changes in the business environment(McNamee & McNamee ,1995). The surface of high profile corporate financial scandals especially in the 1990shas led internal auditors to provide value-adding services and assuming a broader scope of activities including assisting organisations in the management of risk. Today, internal auditing should result in an actionable and value added report that plays a role in the organisation's strategic focus, governance, compliance and effective business processes (Verschoor, 2006).

In 1992, COSO produced a report primarily to address the role of internal controls in achieving improved corporate governance. The report defined internal control as

"A process effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: Effectiveness and efficiency of operations; Reliability of financial reporting and compliance with applicable laws and regulations" (COSO, 1992, pp 9).

The incorporation of 'effectiveness' was the first radical change to the idea of internal control in over four decades. This development shifted the top management's responsibility on internal control from compliance with policies to a focus on important risks and this has put internal auditors at an advantage (Mihret, James and Mula, 2010). By admitting the term "effectiveness" into the ambit of internal control, it recognises the existence of business objectives other than efficiency and probity and this goes some way to aligning the definition with business risk approaches to auditing (Page and Spira, 2002). G. Sarens and I. De Beelde (2006), further added that effective and efficient internal control system enables organisations to respond accordingly to significant business, operational, financial, compliance and other risks.

The Canadian Institute of Chartered Accountants in developing the Criteria of Control Framework (CoCo), provides a definition of control and the criteria for assessing its effectiveness (CICA, 1995). The new definition assumes that controls exist to assist the organizations to manage their risks and promote effectiveness in governance. In 1999, the update of the definition of internal auditing by the IIA to reflect the changes in the work of internal audit departments and by incorporating assurance and consulting services in the new 'internal auditing' definition, have resulted in internal auditing becoming a proactive and consumer focused activity The change in

perspective has considerably broadened the horizons of internal auditing and expanded its working domain, incorporating risk management, control, and governance processes (Chapman & Anderson, 2002). The fulfilment of internal audit functions and organisational objectives would hence extend beyond that of financial assessment with the services that internal auditors provide can be seen to revolve around the achievement of business objectives (Bou-Raad, 2000).

In line with the changing role in internal audit, internal auditor found themselves having a multi-faceted role to play in the risk management. Many companies are looking for internal audit to support strategic business objectives which include ERM activities such as risk identification and prioritisation as well as analysis and quantification of risk factors in new ventures and strategies (KPMG, 2007). Verschoor (2006) maintains that a crucial part of the internal auditor's work includes clarifying their roles in assurance and consulting as well as ensuring risk based audits add value.

2.3 ERM and Role of Internal Auditing

The financial and accounting scandals in the 90s in US and UK have resulted in the tightening up of corporate governance measures in many countries which included the integration of risk management initiatives as part of the corporate governance code. The internal and external pressures and other risk drivers have also increased the complexity of risk which the traditional risk management is no longer appropriate to identify, assess and respond to (Bearsley, Chen, Nunez and Wright, 2006). The increasing complexity of risks which is identified as one of the factors to have influenced the ERM implementation, has called for internal auditor to develop new skill set (KPMG, 2007) and adopt a risk based approach to work.

Figure 2.1 depicts the various ERM drivers based on the literature review (Miccolis & Shah, 2000; Davenport & Bradley, 2001;Rosen & Zenios, 2001;Lam, 2003)

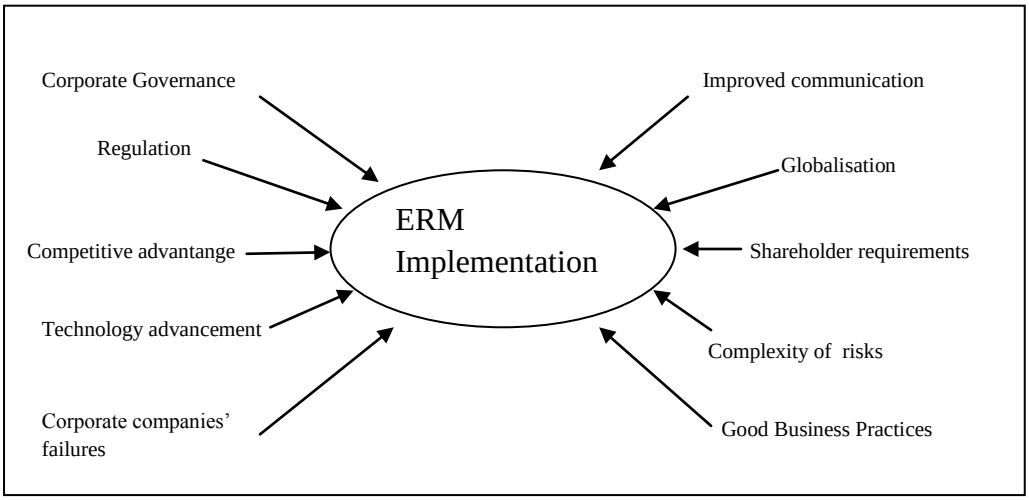

Figure 2.1 ERM Drivers

With the heightened concerns on risk management, there is a need for a framework that is robust to identify, assess and manage risk effectively (Flaherty, 2004). It is thought that ERM "provides a solid foundation upon which companies can enhance corporate governance and deliver greater shareholder value" (Bowling & Rieger, 2005). In fact, ERM has been widely recognised as a new paradigm for managing the portfolio of risks facing the organisation (Beasley et al, 2005; O'Donnell, 2005; Banham, 2004) unlike the traditional risk management where individual risk categories are separately managed in risk 'silos' which resulting in an overlapping and excessive costs for organisation as well as failing to provide an overall view of risk reporting to senior managers and boards of directors (Lam, 2000). ERM is a dynamic process that integrates a risk management approach enabling firms to manage and minimize their level of risk (Busman and Zuiden, 1998) and is considered as a tool

which allows organisations to manage their risks in a manner to achieve the greatest gains at the lowest cost (Chapman, 2001).

The improvement of the overall standard of risk management and internal control of listed companies was attributed to the Turnbull Report which was first issued in 1999 (Lam, 2010). Bolton (2000) asserts that Turnbull provides organisations with the opportunity to create a control culture where risk management is embedded as part of day-to-day activities of the organization as well as providing internal auditors with the chance to raise their profile and demonstrate to boards and audit committees their capabilities in assisting the organisation to manage risks. The Turnbull Report was premised on the adoption of risk-based approaches to internal control by corporate boards and on the subsequent monitoring of the effectiveness of the internal control (Fraser and Henry, 2007). This has caused organisations to formalise procedures for risk identification, management and reporting (Fraser and Henry, 2007). One of the key requirement of the Board as the consequence of the Turnbull Report which is incorporated in the Corporate Governance Code, is to gain assurance that the risk management processes are working effectively and that the key risks are being managed to an acceptable level (Matyjewicz and D'Arcangelo, 2004).

In Malaysia, the Malaysian Code on Corporate Governance that was amended in March 2000 incorporates risk management as a principle of corporate governance under Principle of DII in Part I and makes risk management as a principal responsibility of the Board in Best Practice Provision AA1 in Part 2. These principles are included as a listing requirement of the Bursa and are made mandatory to comply with by companies listed in Bursa Malaysia.

With the prominence gained by profession, internal auditors can assist businesses in managing their risks more effectively by identifying problems and suggesting value adding improvements to the organisations (Allott, 1996). However, the extent of internal auditors' involvements in ERM have created much controversy (Banham, 2004). The COSO ERM framework calls on the internal audit function to assist management and board of directors or audit committee in managing their organisational risks by examining, evaluating, communicating and recommending improvements to the entity's enterprise risk management (COSO, 2004). However, by assuming the consulting role in ERM activities, internal auditors may risk having their independence and objectivity compomised. Some argue that ERM should be managed by traditional risk overseers from management disciplines, such as Finance or Insurance and that internal auditors should only be restricted to monitoring of ERM activities.Others believe that the internal audit function plays a vital role in overseeing ERM framework, given the internal audit's natural focus on risks and controls. ICAEW (2000) views the assurance role of internal auditor includes carrying out the assessment on the adequacy and effectiveness of the risk management processes where risks are identified, prioritised, managed, controlled, mitigated and reported. This excludes assessing the appropriateness of company objectives or board strategies (ICAEW, 2000). The requirement for internal auditors to provide assurance on the appropriateness of risk management would lead internal auditors into new territory and implies that a greater depth of understanding of risk which internal auditors may not possess (Fraser and Henry, 2004) and lack of the necessary expertise could present as a weak link in the risk management "chain" (Fraser and Henry, 2007). Piper (2002) is of the view that dedicated chief risk officers or departments should report to boards on risk management

whilst internal auditors should assess and report on the underlying risk management processes. IIA (2004) on the other hand encourages internal auditors be the “champion” for ERM but suggests that their role in this respect should diminish as risk management becomes increasingly embedded. Therefore, there is not clear cut role for internal auditors in ERM (Walker et al., 2002). However, there should be an obvious body within organizations to manage risk and internal auditors or audit committees may fill the gap simply because many risks have an obvious financial dimension (Fraser and Henry, 2007).

Whilst Standards and Practice Advisories issued by IIA encourage involvements of internal auditors in ERM eg. Practice Advisory 2100-3: Internal Auditing ‘s Role in the Risk Management Process and Practice Advisory 2100-4: Internal Auditing’s Role in Organizations without a Risk Management Process, IIA (2004), it has also recognised the impending threats of internal auditors’ involvements in ERM to their independence and objectivity. The need to provide independent assurance raises the question whether risk management should be separated from internal audit as there is a risk that independence would be compromised if internal auditors become too involved in the risk management process (Fraser and Henry, 2007). Due to the surrounding controversy and in the interests of protecting internal audit independence and objectivity, IIA (2004) issued a global position paper, "The Role of Internal Auditing in Enterprise-wide Risk Management," defining the internal auditor’s core roles and involvements in ERM as well as to assist chief audit executives (CAEs) in responding to enterprise risk management (ERM) issues in their organizations.

The paper suggests the roles that the internal audit function should and should not play throughout the ERM process, ranging from full involvement to no involvement. They are *Core Activities* that provide assurance on risk management and according to IPPF, internal auditors can and should perform at least some of these activities; *Legitimate Activities* which principally involve consulting roles in ERM that internal auditing may undertake provided safeguards are exercised on the part of the internal auditors and *Inappropriate Activities which involved* consulting activities that internal audit should not undertake as to ensure that its independence and objectivity are maintained.

The 18 roles identified in the IIA position paper (2004), are divided into 3 categories of ERM-related activities according to the level of responsibility as depicted in figure 2.2 below.

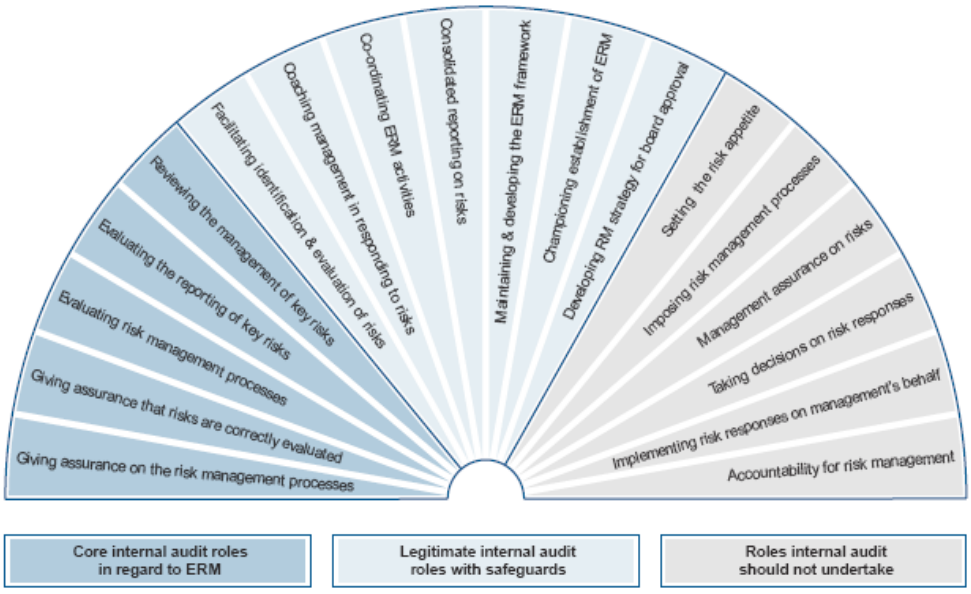

Figure 2.2 Internal Auditing's Roles in ERM (ERM Fan)

In previous studies on internal auditing function in ERM, various findings were noted. Walker et al. (2002) in their study on the role of internal audit in ERM process at 5 leading companies found that heavy involvement of internal audit function in ERM activities in each company with the chief audit executive played a vital leadership role in spearheading the ERM efforts, being the ERM process owner as well as being a risk champion. Allegrini and D'Onza (2003) in their study revealed that, within large Italian companies, internal auditors were involved in risk management activities eg. customizing the risk management methodology to the organization, carried out consulting services in risk management activities or facilitated control and risk self assessments. These findings are further supported in the study conducted by Beasley et al. (2005) which found evidence of internal audit focus on coordinating ERM effort amongst various parties, assisting with risk identifications, suggesting control activities, and monitoring ERM process. Gramling & Myers (2006), on the other hand examined internal audit's role in ERM for conformity with the appropriate internal audit role recommended in the IIA paper (2004) and found that the internal audit's ERM related activities at many organisations appear fairly consistent with IIA guidelines. In a survey of the internal auditing profession in US by PwC (2007), it was noted that a third of the internal audit functions are directly responsible for risk management at their entreprises. Though this highlights the importance of ERM, however by virtue of the responsibility, IA would be unable to provide an independent assessment as to the quality of risk assessments (Verschoor, 2007). Yazid et al. (2008) in their study of the ERM practice in Malaysia, found that ERM practices amongst main board listed companies in Malaysian Bourse are still at early stage with only about 30 percent of the companies involved in ERM.

It is obvious that there have been varying findings from studies conducted by academicians on the roles and involvements of internal auditors in risk management activities of organisations. It is noted that risk management progressively taking a more important position in the corporate governance landscape and this paper seek to examine whether risk based auditing does contribute to the extent of risk management activities which are being adopted across organisation wide.

2.5 Summary of Literature Review

This section overall reviews the existing literature on the risk based auditing approach as well as the internal auditor's function and roles in ERM related activities. The literature reveals that the internal auditing method has evolved to a risk based approach over the years and the regulatory requirements eg. SOX and the financial scandals in the 90s have forced upon the corporations to establish their objectives and identify and manage their risks. Risk based approach which was widely regarded as 'best practice' gradually gained prominence in internal auditor's audit work both at audit planning and individual audit assignment levels as a result. On the other hand, the scope of internal auditing function was found to have increased due to changes in business environment. The internal auditor's role in its current form to a large extent is influenced by the re-definition of internal auditing by IIA (1999) as well as the broadening of the scope of internal control. As a consequence, internal auditing role becoming proactive and focuses on managing of risk and value adding activtities.

The tightening of corporate governance measures largely after the issuance of Turnbull Report in 1999 has seen internal auditors involved actively in ERM activities. These activities though provide organisations with value added services, run the risk of

internal auditors compromising their stance on objectivity and independence. This conflict of interest has called for IIA to issue a position paper in 2004 to serve as a guide to internal auditors and clarified IIA's stance of internal auditor's involvements in ERM activities. Surveys carried out on the extent of internal auditor's involvement in ERM activities have revealed varying findings.

Notwithstanding these revelations, the adoption of risk based auditing method by internal auditor is said to lend itself to their involvements in ERM activities. It is of great interest to establish the association if any between the risk based approach adopted by internal auditors and the extent of their responsiveness to involvement in ERM activities. The findings shall contribute to the ever increasing knowledge gained from the academic researches in this area of study.

We shall follow on with development of the research methodology and hypotheses, outline key variables, report results, engage in discussion, and make concluding remarks in subsequent chapters.