Enterprise Risk Management: A Guide to Its Implementation

Hussain Adedayo SALAUDEEN
Department of Accountancy,
The Federal Polytechnic, Offa,
Kwara State, Nigeria.
salaudeenhussain82@gmail.com

ABSTRACT

This study titled enterprise risk management: a guide to its implementation was carried out with a view to providing an insight into how ERM should be implemented by would be organizations. This study carried out a review of the requirements of regulatory bodies such as Sarbanes-Oxley Act of 2002, guidance of different frameworks like COSO (2004), various acts and report as well as the activities of rating agencies such as Standard and Poor with respect to risk management with the help of qualitative design. The study found that more emphasis was placed on risk governance structure and risk management procedures/processes. With respect to the governance structure, one of the key features is the assumption of far reaching risk management responsibilities by the board and management. On the other hand, risk management philosophy, risk appetite and tolerance sit at the very heart of the risk management processes. The study recommended that setting up risk management goal; establishment of effective risk governance structure; appointment of chief risk officer and setting up of risk management committees; establishment of risk management procedures; training of risk management personnel; implementation of the risk management procedures; and evaluation of risk management activities by comparing the achieved goal with the set risk management goal should be the necessary steps for firms willing to implement ERM.

Keywords: *Enterprise Risk Management, Integrated Risk Management, Silo-based approach, Value-Creation, Chief Risk Officer, COSO 2004, Sarbanes-Oxley Act 2002.*

Introduction

The need for a paradigm shift from the erstwhile traditional risk management model became more apparent in the aftermath of the 2007/2008 global financial crisis. The general believe amongst stakeholders of the probable cause of the crisis was the ineffectiveness of the erstwhile risk management model to curtail banks from taken excessive risks (Ellul & Yerramilli, 2010; Acharya, Philippon, Richardson & Roubini, 2009). Argument against traditional risk model otherwise known as Silo-based model was deep rooted in the inability of the model to manage more complex and interdependent risks associated with modern businesses. In the traditional risk management approach, line managers were made to assume far reaching risk management responsibilities within their functional areas. In this way, response to multiple interrelated and cross-enterprise risks that affect different parts of organization in different dimensions was not properly managed (Beasley, 2019).

The attention has now turn to a more robust risk management approach known as enterprise risk management (ERM), where risk are viewed in aggregation as against silo approach where risks are managed in isolation or on the basis of department, unit or division. ERM has been widely envisioned to provide both resilience and opportunities in the face of uncertainty because arrays of risks facing organizations are managed in an integrated and firm-wide fashion (Linke & Florio, 2019; Hoyt & Liebenberg, 2011). Relying on the notion that ERM increases firm's value, the risk management world has so far experienced a paradigm shift from silo-approach to ERM. The widespread acceptance of ERM

has attracted research attention (Farrell & Gallagher, 2018; Misra, Erik, & Moore, 2019). However, Calls have been made for studies on how firms may implement ERM initiatives because literature is lacking in insight into how ERM should be implemented (Pagach & Warr, 2011; Landsittel & Rittenberg, 2010; Fraser, & Simkins, 2007; Nocco & Stulz, 2006). A study conducted by Beasley, Branson and Hancock (2019), find that COSO Framework, the most used and talked about framework, is seen to be ambiguous and overly theoretical by individuals who are responsible for its implementation. The above situation has created a void in ERM literature. This study was carried out in response to the aforementioned calls.

Literature Review

Enterprise Risk Management (ERM)

There are inconsistencies in the ways the concept is defined as stakeholders have not agreed on a specific definition of ERM (Lundqvist, 2014). Notwithstanding, the definitions as given by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Casualty Actuarial Society Committee on Enterprise Risk Management (CAS, 2003) have been the most prominent among the various definitions with COSO's definition being the widely used in ERM studies (Power, 2009; Lundqvist, 2014; Sithipolvanichgul, 2016).

According to Committee of Sponsoring Organization of the Treadway Commission (COSO 2004), "ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity's objective". On the other hand, CAS (2003) sees ERM as "a discipline by which an organization in an industry assesses, controls, finances, and monitors risks from all sources for the purpose of increasing the organization's short-term and long-term value to its shareholders". What is more common to these definitions is the management of risk in aggregation.

As holistic approach, ERM tends to manage critical risks that can affect the achievement of strategic objectives on a firm-wide basis. This is achieved by creating a portfolio of significant risks and assessing their interactions (Beasley, 2019). The concept of ERM rests on the conviction that modern risks interacts freely with each other, and that this interactions is capable of creating new risks or modified the existing ones. Therefore, it is far better for a firm to create a portfolio of all risks and manage them on firm-wide fashion. ERM also shift risk management responsibility from unit leaders to board and executive with the board assuming far greater risk management responsibilities.

2.1.1 Frameworks for Enterprise Risk Management

While designing and implementing ERM, organizations had relied on conceptual frameworks related to ERM. Viscelli, Beasley & Hermanson (2016) assert that frameworks for ERM, like COSO 2004; International Standard for Risk Management (ISO 31000), 2009 &2018; Casualty Actuarial Society (CAS) 2003; the joint Australia/New Zealand 4360: 2004 standard; KPMG Enterprises Risk Management Framework 2001; Standard & Poor's ERM framework have been designed to provide guidance for organizations planning to implement ERM. However, extant literature has pointed out COSO, ISO 31000 and CAS frameworks as being the predominant ERM frameworks (Linke & Florio, 2019). However, one specific limitation inherent in all of these ERM frameworks is that they are overly theoretical and this has made it difficult for organizations willing to implement them.

Organizations in the same sector might implement their ERM differently because of the openness of these frameworks and because the frameworks lend themselves to different interpretations. According to Lundqvist (2014), ERM is not a straight-forward subject matter because ERM frameworks provide varied ways of conceptualizing ERM model. First, frameworks for ERM are broad in scope, thus providing an endless ways of conceptualizing it. Lack of a definite and accepted pattern or step by step procedure of ERM implementation presents a challenge to firms adopting ERM. Corporations may approach ERM in different ways leading to variation in ERM practice even for firms with similar characteristics.

The study conducted by Beasley, Branson and Hancock (2010), find that COSO Framework, the most used and talked framework, is seen to be ambiguous and too theoretical in nature by individuals

who are responsible for its implementation. Organizations may likely encounter difficulty when considering the implementation of ERM. The question of how should the ERM system looks like, is undoubtedly, a major dilemma to be faced by any firm proposing to implement and practice ERM.

Methodology

The study adopted qualitative research design. In line with this design, the study is more of explanatory because the study was interested in developing new ideas from the existing literature. In an attempt to identify the components of ERM as well as recommending a step-by-step procedure for implementing ERM, this study first analyzed the regulatory requirements such as Sarbanes-Oxley Act of 2002 (SOX), guidance of different frameworks like Committee of Sponsoring Organization of the Treadway Commission (COSO 2004), various acts and report as well as the activities of rating agencies such as Standard and Poor's with respect to risk management. These analyses are necessary for the purpose of understanding the expectations of various frameworks and acts. It is in the understanding of the expectations or requirements that a decent proposition could be made with respect to how ERM firm should look like and by extension, how organization can go about its implementation.

Review of the Requirements of ERM Frameworks and Rating Agencies on Enterprise Risk Management

A rigorous review was first carried out to establish areas where more emphasis had been placed by regulatory bodies, and rating agencies. Two major aspects of ERM- risk governance and risk management procedures were established. In order to guarantee effective risk management, there is a consensus in the literature of the need for: (1) the involvement of the upper echelon in risk management process; and (2) an effective structure that supports the entire process (Monda & Giorgino, 2013). This assertion is basically making emphasis on risk governance and risk management processes.

For instance, Committee of Sponsoring Organization of the Treadway Commission (COSO, 2004), in recognition of the importance of governance in effective risk management, explicitly recommend or suggest that board of directors and management should spearhead the company-wide risk management process. Committee of Sponsoring Organization of the Treadway Commission (COSO, 2004) thus clearly underscores the role of board and management in risk management. The aspect of the definition as given by COSO 2004 which sees ERM as " a process affected by an entity's board of directors and management" has made clear, the intention of the framework with respect to risk governance structure. The board and management are expected to assume risk management responsibility, a sharp deviation from the prior silo model where the line managers were risk owners.

Similarly, Acts such as SOX (2002), codes such as corporate governance for banks and discount houses (2014) also placed premium on risk governance. The role of the board and management on risk management is clearly spelt out. Just like the provision of COSO (2004), SOX (2002) also requires board of directors and management to assume risk management responsibility. By implication, ERM organizations should have well defined risk governance in place, where the board of directors and management shoulder risk management responsibility. However, in practice, board of directors exercise this oversight function through a committee at the board level often called board risk management committee (BRMC). The management on the other hand carries out this responsibility through either chief risk officer and/or risk management committee (RMC).

Having the board and executive assuming risk management responsibility, the presence of BRMC, CRO and RMC are some of the key dimensions of ERM as demanded by relevant frameworks, acts and rating agencies. Studies such as Shenkir & Walker, 2011; Beasley, Frigo, & Litman, 2007; Lam, 2003, have advanced the need for board of directors and top management commitment to risk management processes. On the other hand, studies such as Segal, 2011; Frigo & Anderson, 2009; Moeller, 2007; Lam, 2003; and Liebenberg & Hoyt, 2003, have also advocated for the appointment of Chief Risk Officer, having a dedicated and independent ERM group or team to support CRO's job.

Furthermore, with regards to the second aspect of ERM which is risk management procedures or process, COSO (2004), CAS (2003), Code of Corporate Governance for public Companies in Nigeria (2014), and Code of Corporate Governance for Banks and Discount House (2014) require that risk

management activities be centrally coordinated as against fragmentation of risk management activities as it is the case of silo model. The centralization ideation of risk management activities requires that a dedicated unit, department, committee or individual be formulated or appointed as the case may be to coordinate risk management processes. Specifically, Code of Corporate Governance for public Companies in Nigeria, 2014 and Code of Corporate Governance for Banks and Discount House, 2014 requires that board establishes a board level risk management committee who will be responsible for risk management oversight on behalf of the board. They also encouraged the appointment of a CRO and constitution of executive level risk management committee. However, the presence of CRO and the constitution of relevant committees are not sufficient if the board and management do not attach importance to ERM activities of the entity.

It is therefore, pertinent that high level executive and board members be appointed to coordinate the risk management processes. The appointment of a high level executive member as CRO and or risk management committee is an indication of the importance the board and management attached to enterprise risk management activities and which, will in turn, guarantees management support of the whole risk management process. Without board and management support, ERM will fail as its success is partly tied with the seriousness with which it receives from the top management (Bowling & Rieger, 2005; Felekoglu & Moultries, 2014; Mensah & Gottwald, 2016).

Accordingly, COSO (2004) stretched the importance of risk appetite in ERM. Equally, frameworks, researchers and practitioners have consistently emphasis the importance of risk appetite in the success of ERM (Ludqvist, 2014; COSO, 2004). Given the strategic position of risk appetite in the success of ERM, it should be one of its dimensions. Thus, an ERM-firm needs to have a formal statement on risk appetite.

Another important dimension is the application of ERM in strategy setting. Ha Do, Railwaywalla, Thayer (2016) argue that application of ERM to strategy setting of firm is key if the former is to achieve the much needed result of value creation. According to Beasley *et al* (2019), "effective ERM should be a valued strategic tool". The proactiveness of ERM system allows for timely identification of emerging significant risks. Insights about potential risks emanating from ERM system would assist management in designing strategy for the organization. The ability of an organization to successfully implement its strategy depends on its ability to apply ERM in strategy setting (Beasley *et al*, 2019; Ha Do, Railwaywalla & Thayer 2016).

Flowing from the arguments and requirements from the various frameworks, acts, and researchers, this study proposes the following as ERM dimensions- board and executive assuming risk management responsibility (this will ensure top level management commitments), the presence of CRO, executive director ERM or their equivalent (to ensure independent risk management function), the existence of board risk management committee and executive level risk management committee, statements on risk appetite, and the application of ERM to strategy setting. Therefore, an ERM-firm must have the above dimensions in addition to other characteristics such as risk identification, risk assessment and risk response, which are also applicable to other risk management models other than ERM.

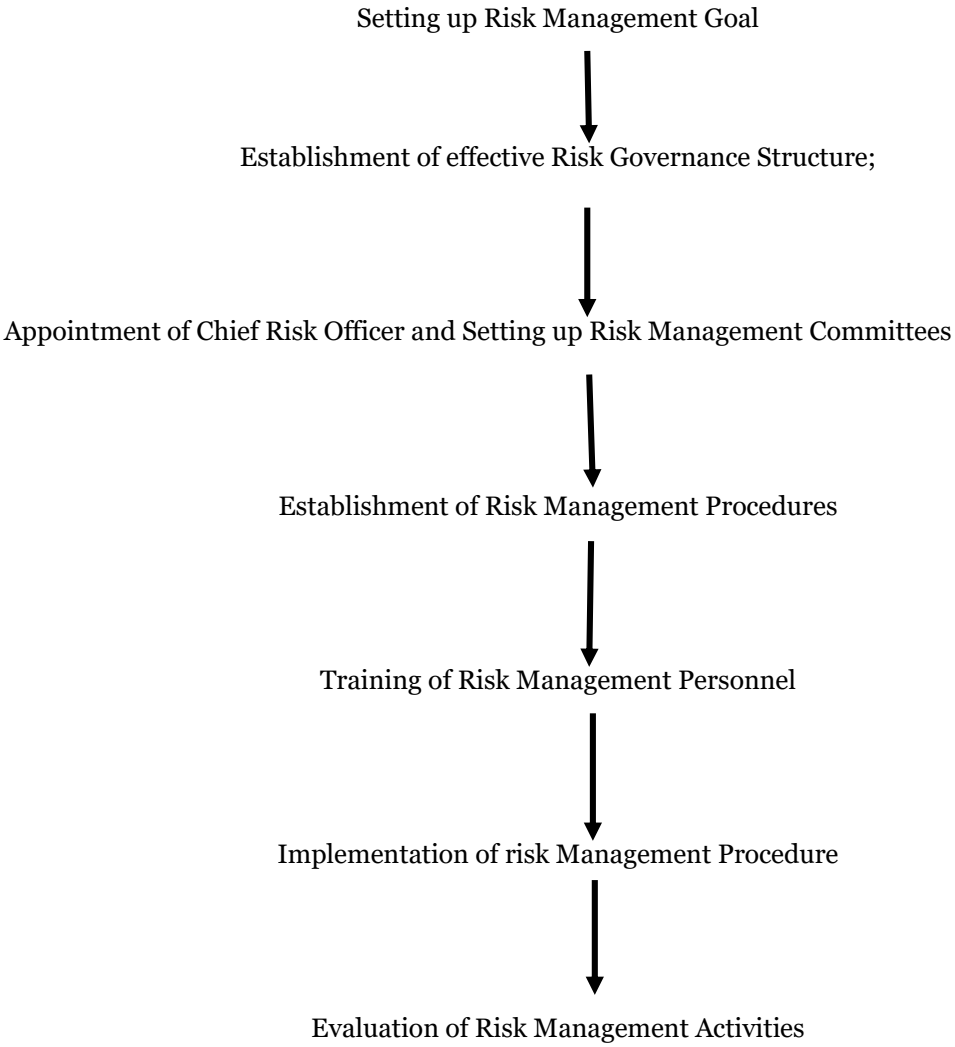
Conclusion

The study concluded that more emphasis has been placed on risk governance structure and risk management procedures/processes. Board and the management now assume far reaching risk management responsibilities. On the other hand, risk management philosophy, risk appetite and tolerance sit at the very heart of the risk management processes

Recommendation

The study recommended the following steps in the implementation of ERM: setting up risk management goal; establishment of effective risk governance structure; appointment of chief risk officer and setting up of risk management committees; establishment of risk management procedures; training of risk management personnel; implementation of the risk management procedures; and evaluation of risk management activities by comparing the achieved goal with the set risk management goal.

Appendix
Step-by-Step Implementation of ERM



Source: Author's Review, 2023

References

Acharya, V. V., Philippon, T., Richardson, M., & Roubini, N. (2009). *The financial crisis of 2007-2009: Causes and remedies*. Wiley, Finance.

Bailey, C. (2019). The relationship between chief risk officer expertise, enterprise risk management (ERM) quality, and firm performance. *Journal of Accounting, Auditing & Finance*, 37(1), 1-25. https://doi.org/10.1177/0148558x19850424

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2019). The state of risk oversight: An overview of enterprise risk management practices. *ERM Professional Insights, 10th Anniversary edition, spring 2019*.

Beasley, M. S, Frigo, M. L. & Litman, J. (2007). Strategic risk management: Creating and protecting value. *Strategic Finance*, 88(11*),* 24–35.

Bowling, D. M., & Rieger, L. (2005). Success factors for implementing enterprise risk management. *Bank Accounting and Finance, 18(3), 21-26*.

Casualty Actuarial Society (CAS, 2003), Overview of Enterprise Risk Management. *Casualty Actuarial Society Enterprise Risk Management Committee*.

Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004). Enterprise Risk Management-Integrated Framework. https://doi.org/10.1504/IJISM.2007.013372

Ellul, A., & Yerramilli, V. (2010). Stronger risk controls, lower risk : Evidence from U. S. Bank Holding Companies. *AXA Working Paper Series No 1, Discussion Paper No 646*.

Erin, O., Eriki, E., Arumona, J. & Jacob, A. (2017). Enterprise Risk Management and Financial Performance: Evidence from Emerging Market. *International Journal of Management, Accounting and Economics*, *4*(9), 937–952.

Farrell, A. M., & Gallagher, R. (2018). Moderating influences on the ERM maturity- performance relationship. *Research in International Business and Finance*, 1-29. https://doi.org/10.1016/j.ribaf.2018.10.005

Felekoglu, B., & Moultries, J. (2014). Top management involvement in new product development: A review and synthesis. *Journal of Product Innovation Management,31(i), 159-175*.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *British Accounting Review*, *49*(1), 56–74. https://doi.org/10.1016/j.bar.2016.08.003

Fraser, J. R., & Simkins, B. J. (2007). Ten common misconceptions about enterprise risk management. *Journal of Applied Corporate Finance*, 19(4), 75-81.

Frigo, M. L., & Andrson, R. J. (2011). Embracing enterprise risk management : Practical approaches for getting started. *ERM Initiative Faculty, Pole Collee of Management*.

Ha Do, Railwaywalla, M., & Thayer, J. (2016). Integration of ERM with strategy: Case study analysis. *Poole College of Management, ERM Initiatives*.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management: Evidence from the U. S. Insurance Industry. *Journal of Risk and Insurance*, *78*(4), 795–822.

Lam, J., (2003). Enterprise Risk Management: From Incentives to Controls. John Wiley & Sons, Inc., Hoboken New Jersey.

Landsittel, D., & Rittenberg, L. E. (2010). COSO: Working with the Academic Community. *Business Accounting Horizons, 24(3), 445-469*.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk management and insurance review*, *6*(1), 37-52.

Linke, A., & Florio, C. (2019). Enterprise risk management: Insight from an interdisciplinary literature review. In Linsley, P., and Wieczorek-Kosmala, M. (eds) Multiple perspectives in risk and risk management. Springer Proceedings in Business and Economics.

Mensah, G. K., & Gottwald, W. D. (2016). Enterprise risk management: Factors associated with effective implementation. *Risk Governance and Control, 6*(41), 175–206. https://doi.org/10.22495/rcgv6i4c1art9

Misra, B. K., Erik, R. A., & Moore, M. (2019). A framework for enterprise risk identification and management: The resource-based view. *Management Auditing Journal, 34(1),* 62-88.

Monda, B., & Giorgino, M. (2013). An ERM maturity model. ERM symposium monograph.

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and Practice. *Journal of Applied Corporate Finance*. https://doi.org/10.1111/j.1745-6622.2006.00106.x

Pagach, D. & Warr, R. (2007). The characteristics of firms that hire chief risk officers. *Journal of Risk and Insurance*, *78*(1), 185–211.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*, 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Shenkir, W. G., and P. L. Walker. (2011). *Enterprise Risk Management: Frameworks, Elements and Integration*. Montvale, NJ: Institute of Management Accountants.

Sithipolvanichgul, J. (2016). Enterprise risk management and firm performance: Developing risk management measurement in accounting practice (Doctoral Dissertation, University of Edinburgh)

Viscelli, T. R., Beasley, M. S., & Hermanson, D. R. (2016). Research Insights About Risk Governance : Implications From a Review of ERM Research. *SAGE Open*, 6(4). https://doi.org/10.1177/2158244016680230