Enterprise Risk Management – International Standards and Frameworks

Angage Anoma Samanathi Perera

Senior Lecturer, Australian College of Business and Technology, Colombo, Sri Lanka

DOI: 10.29322/IJSRP.9.07.2019.p9130
http://dx.doi.org/10.29322/IJSRP.9.07.2019.p9130

Abstract- Under the massive expansions of the world economies in the recent years, business organizations have realized the significance of integrating risk management into their strategies as the nature of business risks upcoming are terrifyingly increasing due to high competition, continuous technological advancements and changing behavior of customers. International organizations who are interested on risk management have published and revised many standards and frameworks to help practitioners to select the best and appropriate risk management framework comparing the strengths and weaknesses of their entities. This paper presents definitions of the risk, risk management and enterprise risk management terms and the summaries of seven internationally recognized risk management frameworks that are popularly used by corporates and in the academic literature.

Key Words- CAS, COBIT 5 for risk, COBIT 2018, COSO ERM updates, Enterprise Risk Management, ISO 31 000, Risk, Risk Management, S&P, TRM.

I. INTRODUCTION

This paper focuses on reviewing the definitions of risk, risk management and the enterprise risk management given by various scholars and researchers using the deductive research approach. A comprehensive literature survey has been conducted in order to find out the definitions as well as international standards and frameworks that are published and used by the present day decision makers in the risk management arena.

The core of the modern economy is the proper understanding of the nature of risks, the art and the science of making correct choices as every choice, from day-to-day operational decisions to the fundamental trade –off decisions made in the board room in order to pursuit the objectives of the firm are involved with a variety of risk types (COSO, 2017). Rubino state that risk and uncertainty bring not only the negative outcomes but also the positive outcomes to an organization. Therefore, firms cannot survive and create value to their stake holders unless they take the risk as a part of their business (2018).

Risk management is hardly a new concept though the principles and application if risk management have arisen since possibly in the 17th century in Europe (Sum, 2017). The origin of the risk management and the practice of risk management started in ancient days where the existence of human beings. In the business context, during the period of 1950s, the insurance industry initiated the use of risk management as many businesses tried to reduce possible hazards through insurance in the US. Later, in 1960s, the concept of contingency planning emerged as an essential tool in risk management as insurance was not sufficient to safeguard the assets of a firm, to control the business operations and to protect the complete loss from risky acts. (Sithipovanichgul, 2016; Li et al, 2014; Farrell & Gallaghar, 2014; Vollmer, 2015). The concept of Traditional Risk Management (TRM) then became popular as a silo base approach in risk management where organizations view each risk type individually and act on them as a stand-alone object. Alawattegama state that TRM is a less effective system for managing risk as each risk is addressed case by case to identify and assess the impact onto organizations with the major concern of mitigation of the risk establishing risk limits but, not to utilize the risk for value creation. Due to many limitations of TRM, the concept of Enterprise Risk Management (ERM) emerged later as a holistic and integrative approach in risk management which will unify all the risk types and integrate them into the overall objectives of the organization. ERM gained the attraction of the modern corporate world as an effective risk management practice which will create and protect the firm value and the stability of the firm in the long run (2018). ERM added a paradigm shift to the risk management arena allowing firms to assess their risk attitude, identify and prioritize risk and identify the risk as acceptable, mitigated or completely avoided. The major focus of ERM is the development of a strategy for the firm enabling the adoption of ERM best practices with the support of all the relevant stake holders (COSO, 2017; Sithipolvanichgul, 2014).

All organizations need to set strategies and review them periodically in order to grab the ever-changing opportunities in the market place for value creation of their firms while managing the challenges expected to occur in pursuit of that value. Therefore, a need has arisen for the implementation of best possible ERM framework for every organization for optimizing strategy and performance for untangling the art and science of making well informed decisions (COSO, 2017).

1.1 Benefits of effective implementation of ERM

According to the World Economic Forum (WEF), in the rapidly changing dynamic environment, the future businesses are expected to be full of volatility, uncertainty, complexity and ambiguity. Every business firm regardless the size or the type of business therefore will have to exhibit traits that drive an effective response to changes (IRM, 2018b).
COSO (2017) framework stresses the following benefits of effective implementation of ERM into a firm.

- ***Increasing the range of new business opportunities:*** management is able to identify new opportunities and related challenges through the ERM framework considering both positive and negative aspects of risk.
- ***Identifying and managing entity-wide risk:*** every part of the business exposes myriad risks that will affect the entire organization. Risk may originate in one department may have inverse effect onto the other divisions. ERM supports the management to identify the sources of risks and the diverse impacts that are created by them in order to sustain and improve the performances of the firm
- ***Increasing positive outcomes and advantages while reducing negative surprises:*** Effective implementation of ERM facilitates the entities to improve their abilities of identifying risk and establishing appropriate solutions, getting ready for facing shocks and surprises that will make unbearable losses.
- ***Reducing performance variability:*** performance variability occurs when the firm does not achieve the expected targets or outcomes and also when the scheduled targets exceeded. Both scenarios make the firm unrest due to unmanageable situations. ERM supports firms to anticipate the targets accurately in both the scenarios which will enable the firm to put forward proper actions required to minimize the disruptions of not achieving expected targets while utilizing the achieved over-targets through proper contingency action plans on managing overall need of resources, prioritizing resource deployment and enhancing resource allocation effectively.
- ***Enhancing enterprise resilience:*** the ability of an entity on accurately anticipating the future changes and ability of planning how firms are responding to these changes may decide the medium and long-term viability of that entity. Effective ERM provides the platform for the entity basically for the survival and also the guidelines for thriving the business into success.

In addition to the above benefits, the implementation of an ERM framework is the best tool for an entity as ERM facilitates the management for the selection of the most suitable strategy to their entity analyzing the risk factors aligning with resources with the mission and the vision of the entity in running the business successfully means the selection of correct choices and accepting trade-offs (COSO, 2017).

II. LITERATURE REVIEW

The purpose of this paper is to present the findings from the review of literature on the topic of enterprise risk management - international standards and frameworks. The literature survey was carried out mainly using electronic versions of journal articles and research publications. The definitions of risk, risk management and the enterprise risk management and the international standards and frameworks that are associated with the enterprise risk management are presented in this paper.

2.1 Definitions of Risk, Risk Management and Enterprise Risk Management (ERM)

ERM is an integrated risk management process which will cover the overall possible risk types that businesses are vulnerable to face and is applied to mitigate risks (Karaka, Serdar &Senol, 2015). Beals (2015) state that ERM promotes the awareness of the risk factors in the top management and helps them in making decisions. Beals further insists that an effective decision making process increases the performances of the firm while reducing the cost of capital.
ERM has emerged as a holistic risk management approach replacing the TRM silo approach in the last decade realizing the importance of having a proper risk management system in organizations as no more firms can tolerate financial losses causing from unexpected events, disruptions to normal operations, damage to reputation and loss of market presence (IRM, 2018b). Implementation of a proper ERM system enables the firms to improve the decision making process related to strategy formulation where different strategic options are fully analyzed to reach the best strategy and enables the firm to make the risk adjusted tactics. ERM further helps to identify the possible events that will disrupt the operations of the entity and facilitates to reduce the likelihood of these events limiting the loss of occurrence. Compliance area can be enhanced by the implementation of ERM best practices recognizing the statutory and customer obligations well in advance and providing solutions avoiding the possibility of risks associated with those compliance issues (COSO, 2004).

Sithipolvanichgul (2016) expresses that the poor practices of Traditional Risk Management (TRM) were the causes for the recent global business crises and emphasized the need for the implementation of ERM mainly because entities can deal with all internal, external, strategic, operational, compliance and reputational risk types through ERM approach. Pooser cited in Sithipolvanichgul (2016) endorsed the idea that the ERM took the greater attention of the business community since the early 2000s and was doubled after the major financial crises (2008-2009) that destroyed the long-term value of big business giants like Enron. As a result, ERM has been largely given the focus by academic researchers and business practitioners in the recent past as the risk management is a critical business function and an essential tool for the survival of the organization.

Despite the popularity of the ERM as an effective approach in risk management, only a little empirical evidence is available to prove that ERM adds a significant impact to the existing value of the firm. Many research studies conducted to prove the significant impact of ERM implementation on the performances of the firm ended with contradictory outcomes where most of them concluded that no significant, positive relationship between ERM implementation and the firm performance (Alawattegama, 2017 & 2018; Karaka, & Senol, 2015; Barac, 2015).

2.2 International ERM Standards and Frameworks

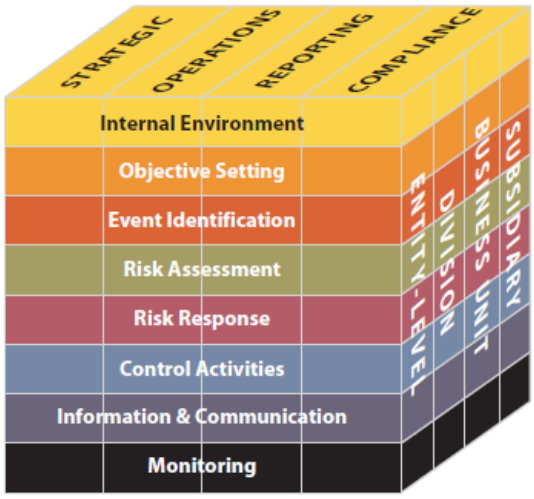
Many definitions and international standards that are associated with ERM have been revealed in this literature review. Rubino (2018) state in his article comparing the ERM standards that though several ERM frameworks are published and revised over time, these standards still have some limitations. Organizations however, if seek to adopt ERM practices into their entities in order to enhance the shareholder's value then will have to choose an appropriate ERM framework beside the limitations. The choice of the suitable framework is based on the experience and knowledge of top management that have gained from internal and external control processes which has made ERM very idiosyncratic (Pundervolt, 2017; Vollmer, 2015).

Principles and guidelines for the correct selection and the effective implementation of the suitable ERM framework are given by various frameworks such as: 1) COSO ERM – Integrated Framework (2004), 2) COSO ERM Integrating with strategy and performance Framework (2017), 3) Casualty Actuarial Society Framework (CAS, 2003), 4) International Standard for Risk Management (ISO 31000, 2009), 5) ISO International Standard for Risk Management (31 000: 2018), 6) COBIT 2019 :Framework of the Information Systems Audit and Control Association for customizing and right-sizing enterprise governance of information technology and 6) Standards and Poor's Enterprise Risk Management: analysis into *Corporate Credit*.

1) Enterprise Risk Management - Integrated Framework by COSO (2004)

The Committee of Sponsoring Organization (COSO) of the Treadway Commission of USA developed this framework updating their two previous versions of *Internal Control-Integrated Frameworks* 1994 and 2001. This framework has eight interrelated components, four categories of objectives and four levels in the enterprise. This framework was developed with the purpose of helping entities to protect the stakeholder value and enhance it with the underlying philosophy of value maximization through risk adjusted strategy and objective formulation (COSO, 2004).

Figure 1.1: Enterprise Risk Management – Integrated Framework developed by COSO (2004)



Source: COSO (2004)

This depiction displays the ability of the firm to focus on ERM implementation as a whole or by categories, components or by units. The effectiveness of the ERM implementation can be judged by assessing the existence and the functionality of the eight components in each department which will give the assurance to the board that the strategic, operational, reporting and compliance objectives of the firm are achieved. These eight components however will not exist identically in every entity due to the size and type of the organizations but may have applications that are more or less complicated and structured (COSO, 2004).

Since the publication, this framework has been successfully implemented by organizations that are in different sizes, different industries and in different countries to identify risk factors, manage those identified risks and to achieve the objectives of the firm (COSO, 2017). Sithipolvanichgul (2016) state that COSO – 2004 framework is the mostly accepted ERM framework by enterprises especially in the accounting literature. Though, this framework was implemented by many firms yet some argued the limitations and the potential for further development to the model. Practitioners suggested to examining some aspects of the framework with more depth and clarity to provide greater insight into the links between strategy, risk and performance (COSO, 2017). Gjerdrum et al as cited in Sithipolvanichgul (2016) state that the COSO 2004 framework is a complex, multi-layered and a complicated model that many organizations found it difficult to understand. Responding to all the arguments and suggestions, Committee of Sponsoring Organizations updated the COSO 2004 framework in 2017.

2) ERM - Integrating with Strategy and Performance Framework by COSO (2017)

This updated version of COSO 2004 framework pays the major emphasis on how ERM informs the strategy and its performance and provides the framework for the board and the senior management of entities in all sizes. It demonstrates how the ERM implementation can accelerate the growth and boom the performance of the firm and contains principles that can be applied in formulation of strategies. This publication consists of two parts as 1) the offering of the perspective on current and evolving concepts and 2) the applications of

enterprise risk management. This framework makes sense for the management, the board of directors or any other governing boards, supervisory boards, board of trustees, other general partners and the owners about the use of enterprise risk management in selecting and refining the suitable strategy for a firm examining the alternative strategies.

The risk oversight role of the board in reviewing, challenging and concurring with management is clearly explained in COSO 2017 framework on establishing suitable strategies and the risk appetite for a firm, aligning the strategies with business objectives, mission and the vision of the firm, making decisions including mergers, acquisitions, funding and dividend-distribution decisions. COSO 2017 further supports in responding to significant fluctuations in firm performances, responding to deviation from core values, approving management incentives and remuneration and maintaining in investor and stakeholder relations.

COSO 2017 framework has five interrelated components covering a set of principles naming 1) governance and culture, 2) strategy and objective setting, 3) performance, 4) review and revision and 5) information, communication, and reporting. There are twenty principles covered by these five components as shown in the figure 1.3 below.

Figure 1.2: Twenty principles under five components of the COSO (2017) framework

Source: COSO (2017)

3) Casualty Actuarial Society Framework (CAS, 2003)

CAS formed an ERM Committee and summarized the ERM process in 2003, taking the Australian/ New Zealand risk management standards (AS/NZS 4360) as the guide lines. The objectives of the CAS framework are similar to the objectives of the COSO (2004) framework and ISO 31 000 frameworks as the major focus of all these frameworks is the maximization of the firm value achieving the set objectives. CAS framework recommends the establishment of an independent risk management structure for implementing the ERM practices into an organization (Sithipolvanichgul, 2016).

4) ISO 31 000: 2009 – The International Risk Management Standards

International Organization for Standards (ISO) is an independent, non-governmental organization established with the purpose of bringing up the experts together to share knowledge and develop international standards to encourage innovations and to provide solutions to global problems, now has a membership of more than 160 national standard bodies (ISO 31000, 2009). ISO 31 000: 2009 version of the standards was developed by the technical committee of ISO on risk management to provide the guidelines and principles for the decision makers revising the Australian/New Zealand risk management standards (AS/NZS 4360) (Javaid & Iqbal, 2017).

ISO 31 000 provides guidelines but not requirements and therefore, it is not intended for certification yet applicable for all the organizations regardless the size, type or activities and locations to manage risk of all types. This framework was developed by a range of stake holders and recommended not only for risk professionals but also for anyone who involves with risk management strategy formulation. The overall goal of this framework is to develop a risk management culture where all the stake holders of the entity are fully aware of the critical importance of monitoring and managing risk. ISO 31 000 provides direction to identify both positive opportunities and negative consequences involved with risk and provides the foundation for making effective, accurate and timely decisions in the resource allocation process. It is an open, principle based system which will enable the organizations to apply these principles and standards matching with the context of the firm. The major strength of ISO 31 000 risk management approach is the ability to identify the risk owners, which is a must for the accountability, proper communication and for implementing training programmes throughout the organization (ISO 31 000:2009).

Gjerdrum as cited in Sithipolvanichgul (2016) state that ISO 31 000 framework provides a concept where risk management is at the center and is linked to the objectives of the organization which will be useful in planning, managing and governance of the corporate. Further, Gjerdrum recommends that it is not necessary for switching to ISO system if an entity has already implemented COSO

framework due to many commonalities in between these two approaches. Aven as cited in Sithipolvanichgul (2016) argues that the definition given by ISO 31 000 for the risk term misinterprets the exact meaning of the risk and mislead the organization to make illogical judgements as there are no any mathematical basis in ISO 31 000 standards and have limited use of probability, data and models. ISO standards are reviewed in every five years to ensure that the principles and guidelines are relevant and update to meet the needs of the market. The revised version of ISO 31 000 was published in 2018 considering the evolutionary changes in the market place and in order to match with the new challenges faced by present day organizations.

5) ISO 31 000: 2018 – A Risk Practitioners Guide

Institute of Risk Management (IRM) published the revised version of ISO 31000 under the name of "A Risk Practitioners Guide to *ISO 31 000: 2018*" reviewing the present day challenges faced by entities in allocating resources for ERM providing guidelines for professional standards related to risk management of all industries, all disciplines and all public, private, for profit or non-for-profit across the world (IRM, 2018b).

ISO 31 000:2018 provides more strategic direction compared to its previous version and emphasize more on involvement of senior management on risk management and integration of risk management into the firms' decision making process. Also, this new framework recommends the development of policy documents clarifying the role of parties involved with risk management such as CRO, Auditors and compliance officer. The new framework highlights the importance of embedding the risk management into the organizational structure, processes, objectives, strategy and daily operations of an entity. ISO 31 000: 2018 framework has streamlined the content of the previous ISO version due to many complains from practitioners and academics about the complexity of the content and the difficulty of understanding the technical terminologies of the earlier version. ISO 31 000:2018 framework has more useful information and provides clear guidelines for entities for the implementation of risk management practices easily. However, it does not provide step-by-step checklist for entities on ERM implementation process and risk management professionals are thereby challenged as they will have to adopt their own approach in implementing the ERM into their organizations (IRM, 2018b).

6) COBIT 5: Complete Business Framework for the Governance of enterprise IT

In this modern era, Information Technology (IT) plays a major role in operations, management and the growth of entities. IT especially shape the existing strategies and open-up new business avenues for organizations while creating and exposing enterprises into new set of threats such as cybercrimes, errors and various vulnerabilities in business processes and technology awareness of people. IT affairs were not much attended by the senior management previously though, today's entities are much more relied on information systems (IS) and as a result it has changed the dimension of the risks coming from information technology increasing the attention of risk professionals (Javaid & Iqbal, 2017).

Control Objectives for Information and related Technology (COBIT), is an internationally recognized IT management framework which contains a set of best practices for IT management developed by Information Systems Audit & Control Association (ISACA) to help IT professionals and enterprise leaders to fulfill their IT Governance responsibilities while creating the value to the business. COBIT helps businesses to develop, organize and implement strategies around information management and governance. COBIT 5 version of the framework was released in 2013 including more information related to risk management and information governance to its' previous versions of COBIT 3 (2000), COBIT 4 (2005) and COBIT 4.1 (2007) (White, 2019).

7) Standards & Poor's and Enterprise Risk Management

Standards and Poor's (S&P) has added ERM component into their credit rating analysis process since 2005, especially focusing the business sectors of Energy, Financial services and Insurance and introduced the same for non-financial sector in 2008. As a result, all financial and non-financial sectors should now focus on risk management culture and the strategic risk management philosophy of their entities in order to achieve a good S&P rating. Companies with good S&P rating have high capacity and greater access to external capital at lower borrowing cost due to the high confidence of the lenders (Sithipolvanichgul, 2016).

The precedence to the real value of ERM given by S&P's classifications create a culture of risk resilience with the ability to adapt to changes. The limitation of S&P's ERM rating is that, it is judgmental the assessment of the effectiveness of the ERM implementation. There is no any indication in the S&P's of any specific ERM framework and the implementation of the same to achieve objectives of the entity but, it mentions the components of effective risk management to be considered when assessing the risk management process of the enterprise (Hampton as cited by Sithipolvanichgul, 2016).

III. DISCUSSION

The terms "risk", "risk management" and "enterprise risk management" have been given various definitions by international standard organizations, academics, researchers and practitioners and there is no universally accepted single definition for these terms. This has made a major confusion and an ambiguity among the practitioners and risk management professionals not having proper, consistent and uniformity in definitions. Therefore, it has risen the need for the development of proper, compatible and comparable international standards for enterprise risk management where any firm regardless the size, the type of business or the industry can commonly apply.

Many enterprise risk management frameworks have been developed by international standards organizations in the last two decades to combat the risk spectrum but, most of these standards focus on large scale businesses where well established systems and processes are in place plus risk management experts are on duty. Most of these international standards are specific for some special business types and provide generic guidelines for the strategic level but not for the operational level (Javaid & Iqbal, 2017).

Hampton states that COSO and ISO ERM standards are the most suitable frameworks to follow and implement ERM though, it is essential for companies to consider the indicators of effective risk management given in S&P's framework. Mikes and Kaplan, Nielson et al., Tahir and Razali indicate that COSO is the most appropriate framework for ERM implementation and therefore have been used by many researchers and practitioners whilst S&P's ERM component is widely used by insurance companies. CAS ERM framework is only used by a few academics in their research studies (as cited in Sithipolvanichgul, 2016).

It is tedious for an enterprise to select the most appropriate risk management framework for the self-organization yet it is the first step of the ERM implementation process. The selection, customization and the application of the matching standards and framework for an entity is a time consuming process with the commitment of an ample amount of resources which is difficult for small organizations to bear. In-depth knowledge is essential about the standards and frameworks as well as the good understanding of the strengths and weaknesses of the entities to consider adhering to any particular standard which requires the service of expert human resource again at high cost. Thus, the implementation/application of international risk management standards are still at a sour level in many organizations because of the poor level of understanding of the top management on the importance of effective implementation of enterprise risk management standards (Rubino, 2018).

IV. CONCLUSION

This paper discussed the terms of risk, risk management and enterprise risk management given by various authors, the benefits of implementing an effective ERM system for an organization, the difference between the traditional risk management and the enterprise risk management and the international standards and frameworks available for organizations to choose the most appropriate framework for their work setting.

The process of selecting and implementing the most appropriate risk management framework for an enterprise is a complex and a time taking activity which varies from company to company. There are many factors influencing this whole process such as the organizational governance culture, the risk philosophy of the entity and the size of the organization.

There is a number of frameworks which is developed by international standards organizations in order to fulfil the need of having consistent and compatible guidelines for organizations to implement effective ERM systems. It is however, many of these frameworks have had some criticism from practitioners and from academics in terms of complexity and impracticality. Therefore, most of the international standard organizations tend to revise the framework periodically to overcome the limitations of the earlier versions and to include new strategies to combat new challenges upcoming in the market place. As a result, Committee of Sponsoring Organizations (COSO) has now developed two versions of their framework with the latest in 2017. International Standard Organization (ISO) has published the latest version of ISO 31000: 2018 adding new set of instructions and guidelines for organizations. Information Systems Audit & Control Association (ISACA) revised the COBIT 5 version in 2019 as a framework for customizing and right-sizing enterprise governance of IT considering the new trends, technologies and security needs into the framework. COBIT 2019 framework helps aligning business goals through linking IT with other functions of the business organization. Mikes and Kaplan, Agrawal and Ansell as cited by Rubino (2019), despite the updates of the frameworks covering the current risk factors, still there is a need for better frameworks in order to implement an effective and accurate risk management process as the existing frameworks are little integrated with the corporate control systems, including strategic planning and management control.

REFERENCES

[1]. Alawattegama, K. K., (2017). The Effect of Enterprise Risk Management (ERM) on Firm Performance: Evidence from Sri Lankan Banking and Finance Industry. *International* Journal *of Business Management.* 13 (1): 225-237. doi:10.5539/ijbm.v13n1p225

[2]. Alawattegama, K. K., (2018). The Effect of Enterprise Risk Management (ERM) on Firm Performance: Evidence from the Diversified Industry of Sri Lanka. *Journal of Management Research.* 10 (1): 75-93.

[3]. Barac, Z., (2015). *Effective direction and control of higher education institutions; An empirical case study of the Croatian private business school*. (Doctoral Dissertation, University of St. Gallen, Switzerland). Retrieved from https://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4393/$FILE/dis4393.pdf

[4]. Beals, S., Fox, C. & Minsky, S. (2015). Why a mature ERM effort is worth the investment. Risk Management and Insurance Society (RIMS) Executive Report. Retrieved from https://www.rims.org/Documents/MatureERM_whitepaper.pdf.

[5]. Committee of Sponsoring Organizations of Treadway Commission (COSO). (2004). *Enterprise Risk Management - Integrated Framework- Executive Summary.* https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

[6]. Committee of Sponsoring Organizations of Treadway Commission (COSO). (2017). *Enterprise Risk Management: Integrating with Strategy and Performance -Executive Summary.* https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf on 14 March, 2019.

[7]. Farrell, M. & Gallagher, R. (2014). The valuation implications of enterprise risk management maturity. *The Journal of Risk and Insurance, 82*(3), 625-657. doi: 10.1111/jori.12035

[8]. Institute of Risk Management (IRM). (2018a). *From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks*. Institute of Risk Management, London. Retrieved from https://www.theirm.org/media/3512521/IRM-Report-Review-of-the-COSO-ERM-frameworks-v2.pdf on 14th March, 2019.

[9]. Institute of Risk Management (IRM). (2018b). *A Risk Practitioners Guide to ISO 31000: 2018.* Institute of Risk Management, London. Retrieved from https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf on 14th March, 2019.

[10]. ISO, 2009. *31000: 2009 Risk management Principles and Guidelines.* Sydney, NSW: International Organization for Standardization. Standards Association of Australia. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

[11]. ISO 31000: *Risk Management.* International Organization for Standards, Geneva, Switzerland. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

[12]. Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *In International Conference on Communication Technologies* (Com Tech), 78-90. Retrieved from https://doi.org/10.1109/COMTECH.2017.806575 https://doi.org/10.1109/COMTECH.2017.806575

[13]. Karaca, S.S. & Senol, Z., (2017). The effect of Enterprise Risk Management on firm performance: A case study on Turkey. (Doctoral Dissertation, Cumhuriyet University, Turkey). Retrieved from https://www.researchgate.net/publication/228230435_The_Effects_of_Enterprise_Risk_Management

[14]. Li, Q., Wu, Y., Ojiako, U., Marshall, A., & Chipulu, M. (2014). Enterprise risk management and firm value within China's insurance industry. *Acta Commercii*, 14(1). http://dx.doi.org/10.4102/ ac.v14i1.198

[15]. Puntervold, H. A., (2017). Reputation Management in Higher Education Institutions: *A Comparative Analysis of Public and Private, Norwegian and American Higher Education Institutions* (Doctoral Dissertation, University of Oslo, United States).

[16]. Rubino, M. (2018). Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance. *International Journal of Business and Management*; Vol. 13, No. 12; doi:10.5539/ijbm.v13n12p203
URL: https://doi.org/10.5539/ijbm.v13n12p203

[17]. Sithipolvanichgul, J., (2016). *Enterprise Risk Management and Firm Performance: Developing Risk Management Measurement in Accounting Practice.* (Doctoral Dissertation, University of Edinburgh, London).

[18]. Sum R. M. & Saad Z. M. (2017). Risk Management in Universities. *Proceedings of the International Conference on Qalb-Guided Leadership in Higher Education Institutions* (pp.128-143). Malaysia: USIM | Universiti Sains Islam Malaysia.

[19]. Vollmer, S. (2015*). 6 steps to manage risks and drive performance*. CGMA Magazine. Retrieved from https://www.fm-magazine.com/news/2015/oct/manage-risks-drive-performance-201513224.html

[20]. White, S.K., (2019). *What is COBIT? A framework for alignment and governance*. Retrieved from https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html on 10th April of 2019.

AUTHORS

First Author – Angage Anoma Samanthi Perera, MBA in Management of Technology (Moratuwa), BSc in Physical Science (Sri Jayewardenapura), Senior Lecturer, Australian College of Business and Technology, anoma.edirimanna@acbt.lk.