# DETERMINANTS OF ENTERPRISE LEVEL INFORMATION TECHNOLOGY (IT) RISK MANAGEMENT AND ITS IMPACT TO FIRM PERFORMANCE: AN EMPIRICAL STUDY OF PUBLIC LISTED COMPANIES (PLC) IN MALAYSIA

**CHO CHING LIANG**

**Research report submitted in partial fulfillment of the requirements for the**

**Master of Business Administration**

**UNIVERSITI SAINS MALAYSIA**

**2015**

## ACKNOWLEDGEMENT

First and foremost, I would like to express my deepest gratitude and greatest appreciation to my supervisor, Dr. Teoh Ai Ping for her guidance, patience, advice and encouragement throughout the whole research project. She has given me the confidence, support and advice for me to move forward throughout the process of completing this project.

In addition, I would like to express my sincere thanks to all the respondents of this research on their willingness to spend their time to involve in this survey.

Last but not least, I am very grateful to my family members, colleagues and course mates for their support and understanding throughout my master studies in University Sains Malaysia.

## TABLE OF CONTENTS

**ACKNOWLEDGEMENT** ..... **i**

**TABLE OF CONTENTS** ..... **ii**

**LIST OF TABLES** ..... **v**

**LIST OF FIGURES** ..... **vi**

**ABSTRAK** ..... **vii**

**ABSTRACT** ..... **viii**

**CHAPTER 1 INTRODUCTION** ..... **1**

1.1 Introduction ..... 1
1.2 Background of the study ..... 1
1.3 Problem Statements ..... 6
1.4 Research Objectives ..... 9
1.5 Research Questions ..... 11
1.6 Definition of Key Terms ..... 12
1.7 Significance of Study ..... 14
1.8 Organization of the Remaining Chapters ..... 17

**CHAPTER 2 LITERATURE REVIEW** ..... **18**

2.1 Introduction ..... 18
2.2 Information Technology (IT) Risk Management ..... 18
2.3 Enterprise Level information Technology Risk Management (ELITRM) ..... 19
2.3.1 Perspective of Information Technology (IT) Risk Management ..... 20
2.3.2 The Fundamentals of the Enterprise Information Technology (IT) Risk Management ..... 21
2.4 Information Technology (IT) Risk Management Plan ..... 22
2.4.1 Information Technology (IT) Risks Identification and Classification ..... 23
2.4.2 Information Technology (IT) Risks Assessment ..... 25
2.4.3 Information Technology (IT) Risks Responses Planning ..... 26

2.4.4 Monitoring of Information Technology (IT) Risks Level……..……27
2.5 Technology- Organization-Environment (TOE) Model ..... 28
2.6 Resource Based View (RBV) Theory ..... 29
2.7 Information Technology (IT) Capability ..... 31
2.8 Information Technology (IT) Governance ..... 33
2.9 Collaboration Capability ..... 37
2.10 Firm Performance ..... 39
2.11 Theoretical Framework ..... 42
2.12 Literature Gap ..... 43
2.13 Hypotheses Development ..... 44
2.14 Summary ..... 54

**CHAPTER 3 RESEARCH METHODOLOGY ..... 55**

3.1 Introduction ..... 55
3.2 Research Design ..... 55
3.3 Unit of Analysis ..... 56
3.4 Population and Sample Size and Sampling Method ..... 56
3.5 Measurement Instrument ..... 57
3.6 Data Analysis ..... 63
3.6.1 Descriptive Analysis ..... 64
3.6.2 Structural Equation Modeling ..... 64
3.6.3 Partial Least Square ..... 65
3.6.4 Measurement Model ..... 65
3.6.5 Structural Model ..... 66
3.6.6 Bootstrapping Method ..... 67
3.6.7 Mediating Effect ..... 67
3.6.8 Goodness of Fit Analysis ..... 70
3.7 Summary ..... 70

**CHAPTER 4 RESEARCH FINDINGS ..... 71**

4.1 Introduction ..... 71
4.2 Sample Profile ..... 71

4.2.1 Respondents' Profile ..... 72
4.2.2 Organization Profile ..... 75
4.3 Descriptive Analysis of Variables ..... 78
4.4 Measurement Model ..... 79
4.4.1 Indicator Reliability ..... 80
4.4.2 Internal Consistency Reliability ..... 81
4.4.3 Convergent Validity ..... 81
4.4.4 Discriminant Validity ..... 83
4.5 Structural Model ..... 86
4.6 Mediating Effect ..... 90
4.7 Goodness of Fit (GoF) ..... 91
4.8 Summary of the Hypotheses ..... 92

**CHAPTER 5 DISCUSSION AND CONCLUSION ..... 94**

5.1 Introduction ..... 94
5.2 Recapitulation of the study ..... 94
5.3 Discussion ..... 97
5.4 Implication of Findings ..... 107
5.4.1 Theoretical Contributions ..... 107
5.4.2 Practical Contribution ..... 108
5.5 Limitations of the Study ..... 109
5.6 Suggestions for Future Research ..... 110
5.7 Conclusion ..... 111

**REFERENCES ..... 112**

**APPENDIX A: COVER LETTER AND QUESTIONNAIRES ..... 126**

**APPENDIX B- SMARTPLS- PLS ALGORITHM REPORT ..... 132**

**APPENDIX C: SMARTPLS – BOOTSTRAPPING REPORT ..... 135**

## LIST OF TABLES

Table 1.1: Definition of Key Terms ..... 12

Table 3.1: Measurement Instrument ..... 58

Table 4.1 Summary of Respondents' Profile ..... 72

Table 4.2: Summary of Organization Background ..... 76

Table 4.3: Descriptive Analysis of Variables ..... 79

Table 4.4: Removed Indicators for the Measurement Model ..... 80

Table 4.5: Convergent Validity of Constructs ..... 82

Table 4.6: Discriminant Validity for first-order construct ..... 84

Table 4.7: Summary of Structural Model ..... 88

Table 4.8: Goodness of Fit…….……..….. 91

Table 4.9: Summary of the Hypotheses Testing ..... 92

## LIST OF FIGURES

Figure 2.1: The Balance Scorecard Link Performance Measures..... 40

Figure 2.2: The Theoretical Framework..... 42

Figure 4.1 Measurement Model..... 85

Figure 4.2 Structural Model..... 87

# ABSTRAK

Tujuan utama kajian ini adalah untuk mengenal pasti factor-faktor yang mempengaruhi pelaksanaan pengurusan risiko teknologi maklumat peringkat organisasi (ELITRM) dan kesannya kepada prestasi organisasi. Organisasi perlu memahami bahawa mereka semakin bergantung kepada sistem maklumat dan teknologi maklumat untuk mencapai objektif perniagaan dan ini teleh memyebabkan organisasi lebih terdedah kepada risiko tentang teknologi maklumat. Model yang digunakan adalah berdasarkan kepada rangka kerja berdasarkan teori RBV and Teknologi-Pertubuhan-Persekitaran (TOE) yang merangkumi keupayaan informasi teknologi maklumat, pentadbiran informasi teknologi maklumat dan keupayaan kerjasama organisasi. Kajian ini menggunakan kaedah penyelidikan kuantitatif di mana borang soal selidik telah diedarkan kepada syarikat tersenarai awam di papan utama Bursa Malaysia dan aata yang diperolehi dianalisis dengan menggunakan alat statistil Smart- PLS. Keputusan akhir membuktikan bahawa semua penentu adalah signifikan dengan ELITRM dan ia mempunyai kesan kepada prestasi organisasi. Akhir sekali, ELITRM juga mempunyai kesan mediasi yang signifikan di antara keupayaan teknologi informasi makmulat, pentadbiran informasi technologi maklumat dan keupayaan kerjasama organisasi. Pemahaman yang menyeluruh tentang kesan keseluruhan risiko teknologi maklumat organisasi akan memberi gambaran kepada pihak agar pengurusan risiko teknologi maklumat memainkan peranan yang penting di mana kajian ini akan menggariskan ELITRM dalam pendekatan holistik dan berstruktur yang mengintegrasikan maklumat pengurusan risiko teknologi di dalam organisasi untuk membolehkan mereka lebih berdaya saing dan seterusnya meningkatkan prestasi organisasi.

## ABSTRACT

The main purpose of this research is to identify the determinants affecting the enterprise level information technology (IT) risk management (ELITRM) implementation and its impact to organizational performance. It is crucial for organizations to understand that they are increasingly dependent upon information systems and underlying on information technology to achieve the business objective and needs and thus firms are more vulnerable to the treats of information technology risk. The conceptual model of this study is based on the resource based view (RBV) theory and Technology-Organization-Environment (TOE) framework which includes the independent variables information technology (IT) capability, information technology (IT) governance and organization collaboration capability. This study used the quantitative research method in which the questionnaires has been distributed to the PLCs of main board of Bursa Malaysia and the data collected was analyzed by using Smart-PLS statistical tool. The result has proven all the determinants were significantly related to ELITRM and there is an impact to organizational performance. Lastly, ELITRM was justified has significant mediating effect between information technology (IT) capability and information technology (IT) governance and organizational performance. The practical contribution of this study help the organizations understand the entire impact of information technology risk on the organization as a whole will give an insight to the management for wise and prudent decision in managing the information technology risk management in which this study will outline the ELITRM model in a holistic and structured approach that integrates the information technology risk management in firms to enhance the firm performance.

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

Information Technology (IT) Risk Management is a fundamental concern of every firm. In order to meet corporate objective and business needs, the organizations are becoming increasingly dependent on information systems (IS) and underlying on information technology (IT). This research is about the about the determinants that influence the Enterprise Level Information Technology Risk Management (ELITRM) by using the Technology-Organization-Environment (TOE) model and outcome of ELITRM implementation to firm performance. Chapter 1 discusses the background of the research and the problem statement. Subsequently this chapter outlines the objectives of study, research questions, definition of key terms of variables and significance of study.

## 1.2 Background of the Study

Public listed companies (PLCs) are the companies that are listed in the stock exchange market in Malaysia PLCs are listed in Bursa Malaysia, formerly known as Kuala Lumpur Stock Exchange (KLSE). Bursa Malaysia is mainly divided into Main Market and ACE market with total of 920 companies as of February 2015. Companies that are listed have been classified into different sectors in Bursa Malaysia which include industrial products, consumer products,

construction, mining, finance, hotels, plantation, trading/services, technology and real estate (Bursa Malaysia, 2015).

Bursa Malaysia plays a significant role in Malaysia economy. World Bank (2012), reported market capitalization of listed companies in Malaysia towards the percentage of Malaysia GDP was 156.66 in year 2012 and value at USD 476.34 billion. History has shown that PLCs were facing a lot of uncertainties and challenges which could deteriorate the contribution of the public listed companies (PLCs) to Malaysia's economy. PLCs are struggling in achieving competitive advantage and maintaining the profits while overcoming market uncertainties and economic downturn. The major drawback in Malaysia's economy can be tracked back on June 1997 to August 1998 where the Kuala Lumpur Composite Index (KLCI) drops by 72% due to Asian Financial Crisis (Chin, 2009). This economic crisis has resulting in the drop of business performance and causing sustainability issues among the companies in Malaysia including the PLCs. Bank Negara reported a sharp decline in GDP of 43.5% to only 28.1% during period of the economic crisis. Latest event of crisis that hit Malaysia economic was in year 2007-2009, along these period companies in Malaysia once again impacted by global financial crisis due to housing bubble in United States in which the KLSE has declined by 39.3% (Bank Negara Malaysia, 2008).

Besides that, the international scandals such as WorldCom, Xerox and the famous one Enron have brought an alarming signal to the world. In the meantime, there are few examples from Malaysia companies that failed to safeguard the shareholders' benefit especially in term of the fraud reporting. Perwaja Steel

would be one of them due to failure of the company in ensuring fair and transparent reporting and cause unauthorized million ringgit of deal. In addition, another Malaysian company Technology Resources Industries Bhd (TRI) impact by forex losses and high rate of borrowing in 1997 that failed to recognize and mitigate risk accurately during the financial crisis happen. The above examples has proven that failure in risk management is one of the main reasons for the collapse of public listed companies in Malaysia in which researched studies explained that the failure in risk management among the PLCs had cause an adverse impact on them. In addition, one-tenth of estimated samples from of public-listed companies on the Bursa Malaysia were failed with severely impacted by poor corporate governance and risk management (Jin, 2001).

In recent year, risk management has evolved into more integrated and comprehensive approach which calls the ERM. ERM involve in high-level oversight the entire risk portfolio of the whole organization and with that aligned to the strategic objectives of the organization. This is different to traditional risk management where different individual managers manage the risks individually. ERM framework is an extension of the COSO (1992) Internal Control Framework utilized to address the needs of a more complete control system and move the organization to a risk management processes with enterprise-wide view of risk rapidly and aligned behaviors and decision making with organizations' culture and strategy which foster project success and delivering business value. The importance and benefits of ERM in managing the portfolio of risks that face by the firms has been widely recognize nowadays (Liebenberg & Hoyt, 2003; Aabo & Skimkins, 2005; Nocco & Stulz, 2006).

Malaysia has become one of the information technology hubs in the Asia region (Internet World Stats, 2014). A survey showed that information technology spending in Malaysia is expected to reach US$5.6 billion in 2013 with the increased by 7% compare to the year before (Market Research, 2013). Government of Malaysia announced to invest and develop Digital Malaysia Master Plan for Malaysia's ICT sector in the year of 2012 (Market Research, 2013). It has proven that information technology plays a significant role in the business environment to enhance organizational performance and this master plan can help stimulate organizations to focus in ICT development for expanding the business. In addition, business intelligence which aids the decision making has become more prevalent in organizations nowadays. It is expected that business intelligence software sales increase 9% from 2012 and hit RM114.5 million (US$37 million) in 2013 According to Gartner Research (2013). IT consists of the information system and computer technologies. The former can be includes related information which business processes and functions depends on the other hand the latter is software and hardware that support the storage, processing and distribution of data and information. In Malaysia, 51% of organizations nowadays are increasingly depending on information systems (IS) and information technology (IT) as well as invested business intelligence system for making a better decision, gain competitive advantages of agility, flexibility response to changing environment in order to meet their business and achieve their corporate objectives (Ong, & Siew, 2013). Offering high quality services is evident and hence there is need for implementing widely applicable information system (IS) best practices standards and methodologies. The issue of managing the IT risks becomes less of a technical problem, and more of the problem of

whole organization (Spremić, 2009). In the meantime, the risks associated with intensive use of information system and information technology to improve and support business processes and business as a whole is called the IT risks. As the intensive and widely use of IS and IT in the organization could cause undesired or unexpected misuse, losses and damages in whole business model and its environment which put the organization in threats and dangers. The successfulness of all business activities in an organization in which efficiency, effectiveness of the organization greatly depend on the functions of the IT and IS and a sound risk management process need to focus on executive management and environment frameworks and not just only include technical or operational factors. Therefore, stakeholders for organizations need to analyze the risk correctly, establish level of the risk and subsequently take correct actions to overcome it. This particular paper will stress the importance of information technology (IT) capability, information technology (IT) governance, and organization collaboration capability in a sense of enterprise level which enable organization to achieve their corporate goals and business needs. A comprehensive holistic model that has been proposed in this paper may be the useful tool in managing IT risk level in which enterprise level information technology (IT) risk lies upon and will result in up lifting the organizational performance which determines long term sustainable of the organization in a competitive environment (Ebrahimpour, Salarifar & Asiaei, 2012).

## 1.3 Problem Statement

Information Technology (IT) is pertinent for the sustainability and to support the growth of the business in an organization (Law, C. C., & Ngai, E. W., 2005; Qureshil, S., Kamal, M., & Wolcott, P., 2009). A survey shows Malaysia information technology (IT) spending is expected to reach US$5.6 billion in 2013 with an increase of 7% compare to year before (Market Research, 2013). On the other hand with a bigger picture, according to the latest forecast by Gartner (2014), worldwide IT spending is projected to increase spending of $3.7 trillion in year 2013 and breach total $3.8 trillion in 2014 which is a projected of 3.1 percent increase. From the survey, we can see company has invested huge amount into IT as IT creates the potential to maintain existing business strategies, but also to create new strategies (Van Grembergen, 2004).

IT Risks represent the likelihood that a particular potential vulnerability in certain circumstances with given threat-source can exercise and negatively impacts either he IT assets which includes data, software, and hardware or IT services, key business processes or in the worst case the whole organization. IT risk management is the process of understanding and responding to factors that may lead to a failure in the availability, confidentiality, authenticity, non-repudiation or integrity of an information system. Information security or governance program able to help organization to measure the IT risk level and provides the management processes, technology and assurance to allow businesses management to ensure business transactions and information exchanges between all parties which includes enterprises, customers, suppliers, partners and regulators can be trusted meaning the information is authenticity and

nonrepudiation. Secondly, IT risk management ensure the availability which IT services are available and usable and appropriately resist and recover from failures due to disaster, errors or deliberate attacks. Next, with the present of IT risk management, the completeness, accuracy and validity can be maintained in which information is protected against unauthorized modification and integrity of the information can be achieved. Lastly, ITRM will ensure critical confidential information is withheld from those who should not have access to it (Spremic, 2012). Although IT risks characteristics dramatically change in recent decades, IT is still often mistakenly regarded as a separate organization of the business and thus a separate risk, control and security environment. Today IT risk may affect the corporation's competitive position, strategic goals and in turn the firm performance while since 10 or 15 years ago an IT risk could only cause minor technical problems. For example, Amazon.com would cost the company to lose $600 an hour in revenue and Cisco's would lose $70 million in revenues if systems were down for a day (Nolan and McFarlan, 2005) and not to mention indirect costs and reputation risk at stake. It is estimated that IS downtime put direct losses banking industry at $2.1 million per hour, e-commerce operations $113 and brokerage operations at $4.5 million per hour. Another study on fortune 500 companies shows an estimated average losses of these companies is about $96 per hour due to the IS downtime (Goldstein, 2009).

Performances of Malaysia PLCs are significantly impacted by unanticipated challenges events in the business environment. Thus, it is pertinent that PLCs have to leverage on IT and IS in order to sustain the performance. Thus, PLCs have been investing massive amount of money in IT so that they highly dependent on IT so that they are able to achieve competitive advantage which

could result in increase their business performance. However, highly depending on the uses of IT will lead the companies subject to various IT risks, so a sound IT risk management a pertinent component in sustaining the PLCs organizational performance. Objectives of IT risk management is to protect the companies from internal and external threats and to secured IT assets, such as software, hardware, data and facilities and subsequently, mitigate the losses by implementing the combination of protection measures (Rainer, 1991). Moreover, PLCs must prepare and have the awareness of threats in the uncertain environment. They have to possess their own capabilities and resources in order to identify and respond to the threats effectively. Their business strategies and processes have to be agile to enable them to achieve competitive advantage. Organizations have to be more proactive and they must react accurately to the opportunities and challenges derived from the business pressures, so that they are able to survive and to achieve competitive advantage over other competitors in the industry.

Ineffective information technology governance with insufficient visibility into IT infrastructure and processes, weak internal control and collaboration in companies will resulting in to poor performance due to the failure alignment of IT execution with business goals and strategies further causing the project failure, traceability and accountability issue. (Bowen et al, 2007 and James Roger, 2014) A series of corporate scandals like Enron, Worldcom and EBS International have brought attention into corporate governance mechanisms and the effectiveness of these mechanisms. IT plays a pervasive role in creating value into business strategies, effectiveness in managing IT resources and minimize IT failure while

utilizing IT to improve relationships between organization, customers and suppliers.

In addition, based on the previous empirical studies as well as literature reviews, there are essentials for implementing information technology (IT) risk management from the perspective of firms' performance and sustainability but just outline the information technology (IT) risk management in silo of business process. Furthermore, overview of literature about the information technology (IT) risk management found that most of the articles either discussed about the critical success factors of enterprise or information technology (IT) risk management adoption or the business values brought by information technology (IT) risk management and its impact. There were few articles elaborating the determinants of adoption as well as its impact on the firm performance.

## 1.4 Research Objectives

The aim of this study is to investigate the determinants of the Enterprise Information Technology Risk Management among the public listed company (PLCs) in Malaysia and out its outcome on firm performance in terms of financial and non-financial aspects. Specifically, the objectives of this study are:

I. To examine the relationship between organizations information technology (IT) capability and enterprise level information technology (IT) risk management implementation.

II. To examine the relationship between organizations information technology (IT) governance and enterprise level information technology risk management implementation.

III. To examine the relationship between organizations collaboration capability and enterprise level information technology (IT) risk management implementation.

IV. To examine the relationship between organization information technology (IT) capability and organizational performance among public listed company (PLCs) in Malaysia.

V. To examine the relationship between organizations information technology (IT) governance and organizational performance among public listed company (PLCs) in Malaysia.

VI. To examine the relationship between organizations collaboration capability and organizational performance among public listed company (PLCs) in Malaysia.

VII. To examine the mediating effect of enterprise level information technology (IT) risk management on the relationship between organizations information technology (IT) capability and organizational performance among public listed company (PLCs) in Malaysia.

VIII. To examine the mediating effect of enterprise level information technology (IT) risk management on the relationship between organizations information technology (IT) governance and organizational performance among public listed company (PLCs) in Malaysia.

IX. To examine the mediating effect of enterprise level information technology (IT) risk management on the relationship between

organizations collaboration capability and organizational performance among public listed company (PLCs) in Malaysia.

X. To examine the relationship of enterprise level information technology (IT) risk management implementation and organizational performance among the public listed company (PLCs) in Malaysia.

## 1.5 Research Questions

In order to attain the said objectives as mentioned above, the objectives are transformed into the research questions as follow:

I. Is there a relationship between organizations information technology (IT) capability and enterprise level information technology (IT) risk management implementation?

II. Is there a relationship between organizations information technology (IT) governance and enterprise level information technology (IT) risk management implementation?

III. Is there a relationship between organizations collaboration capability and enterprise level information technology (IT) risk management implementation?

IV. Is there a relationship between organizations information technology (IT) capability and organizational performance among the public listed company (PLCs) in Malaysia?

V. Is there a relationship between organizations information technology (IT) governance and organizational performance among the public listed company (PLCs) in Malaysia?

VI. Is there a relationship between organizations collaboration capability and organizations performance among the public listed company (PLCs) in Malaysia?

VII. Does enterprise level information technology (IT) risk management implementation mediate the relationship between organizations information technology (IT) capability and the organizational performance among the public listed company (PLCs) in Malaysia?

VIII. Does enterprise level information technology (IT) risk management implementation mediate the relationship between organizations information technology (IT) governance and the organizational performance among the public listed company (PLCs) in Malaysia?

IX. Does enterprise level information technology (IT) risk management implementation mediate the relationship between organizations collaboration capability and the organizations performance among the public listed company (PLCs) in Malaysia?

X. Is there a relationship between enterprise level information technology (IT) risk management implementation and organization performance among public listed company (PLCs) in Malaysia?

## 1.6 Definition of Key Terms

In order to have a mutual understanding about the terms used in this study, the following key terms defined and referred throughout this study accordingly.

Table 1.1 *Definitions of Key Terms*

| Constructs | Definition | Source |
|---|---|---|
| Risk | Risk is the degree of uncertainty on a future event and is a phenomenon by definition and nature in which it cannot be eliminated. | Fabozzi & Peterson (2003) |
| Information Technology (IT) Risk | IT Risks is the likelihood exercise of a particular potential vulnerability and negatively impacts the IT assets IT services, key business processes or the whole organization in certain circumstances by a given threat-source | Spremic (2012) |
| Enterprise Level IT Risk Management | A holistic and structured approach that aligns IT resources, IT infrastructure, key resources, governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing risk and uncertainties the organization faces. | Spremic (2012) |
| IT Risk Management Plan | The process of risk management usually consists of risk identification, risk analysis, risk response planning and risk monitoring and control | Hillson (2002) |
| IT Capability | The level of readiness pertaining to technological competency and infrastructure available to the organization including software, hardware, human capital and data collection/integration such as operating system at client and | B. Pudjianto, et al., (2011) |

| | | |
|---|---|---|
| | server level, network connectivity, storage devices for database, user knowledge and data input flow. | |
| IT Governance | The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains to achieve company strategies and objectives | Gartner (2013) |
| Collaboration capability | Collaboration capability refers to the ability of connecting people to work together, build and manage relationships as well as interaction with other individual, team, intra-organizational and inter-organizational. | Lew, Ong & Eze, (2013) |

## 1.7 Significance of Study

This research identifies the determinants for the enterprise level information technology risk management (ELITRM) implementation among the public listed company in Malaysia as well as its impact on the firm performance.

Past studies have shown the information technology (IT) risk management is a crucial to an organization. However, most of the companies do not equip with an up-to-date and tested risk management method (Bowen et al, 2007 and James Roger, 2014). In addition, organizations are more technology-dependent and thus

more vulnerable to the treats of IT risk nowadays. Therefore, stakeholders for organizations need to analyze the risk correctly, establish level of the risk and subsequently take correct actions to overcome it. IT managers working with the respective departmental in the company have to identify different level of IT risk, as well as the vulnerability of the IT assets towards these risks.

This research is interested in public listed company in Malaysia and this study has practical contribution in helping the organization and in this study the PLCs in Malaysia in understanding of entire impact of IT risk on the organization as a whole will give an insight to the management for wise and prudent decision in the process of information technology (IT) risk management (ITRM) and its impact to the organizational performance. Based on the previous empirical studies as well as literature reviews, there are essentials for implementing information technology (IT) risk management from the perspective of firms' performance and sustainability but just outline the information technology (IT) risk management in silo of business process. This study will outline Enterprise Level IT Risk Management Model (ELITRM) in a holistic and structured approach that integrates the information technology (IT) risk management as enterprise wide.

In terms of theoretical sense, this study underlines the resource-based view (RBV) in examining the ELITRM implementation and organizational performance. ELITRM implementation is able to help the firms achieve advantage and enhance the organizational performance in which accordance to RBV, ELITRM implementation will be view as valuable intangible elements for the firms. Furthermore, overview of literature about the information technology

(IT) risk management found that most of the articles either discussed about the critical success factors of enterprise or information technology (IT) risk management adoption or the business values brought by information technology (IT) risk management and its impact. There are few articles elaborating the determinants of adoption as well as its impact on the firm performance. In fact, there is even limited research that examines the pre and post implementation of information technology (IT) risk management with the TOE framework. TOE model is one of the influential and reliable models regarding technology adoption because it is based on strong theoretical background while it is proven and supported by many empirical studies (Oliveira & Martins, 2011). Thus, this research attempts to analyze the collected data within TOE framework. Hence, the result of this learning will become the benchmark for Malaysia public listed companies. The identified factors will contribute to the awareness to those practitioners about building a strong implementation process and reduce the number of failures. The current model in this study is anticipated to be consistent with the TOE model to examine the determinant influencing the ELITRM implementation.

## 1.8 Organization of Remaining Chapters

This report of the research study is organized and presented in 5 Chapters:
Chapter 1: Introduce the background, objective and problem statement of this research and discussed the significance of the study.

In Chapter 2: Identified the related theories, present the literature reviewed and models of this research. The research framework and the variables of this research study will also be identified.

Chapter 3: Mainly focus on research design of the study, methodological procedures and the method of analysis.

Chapter 4: Data analysis will be conducted and results will be present and discussed .Research hypothesis will be tested and explained.

Chapter 5: Conclude the research study with discussion, impact and limitation of the study as well as suggestion for future research.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

This chapter will outline the literature that has been published from the past researches. The first part of this chapter will discuss about the definition and details elaboration of the Information Technology Risk Management in the enterprise environment from different authors. This chapter will also present the literature pertaining to the possible factors determining the Enterprise Level Information Technology Risk Management such as information technology (IT) capability, information technology (IT) governance and organization collaboration capability. Subsequently, this chapter will present an overview literature on the ELITRM and firm performance (financial and non-financial) and the underlying Resource Based View (RBV) and contingency theory. Lastly, this chapter will bring up the gap of the literature and the hypothesis development of this research.

## 2.2 Information Technology (IT) Risk Management

Organizations on information technology (IT) have increased rapidly in heavily technology dependent. Therefore, IT has play an important role in organization ranging and IT personnel have to identify and deal with the risks to IT data and systems, by reducing, avoiding or mitigate as well as to develop a

plan to prepare for uninvited IT crisis. IT risk comprises of software and hardware failure, spam, viruses, human errors, as well as other natural disasters such as floods, fires or cyclones (Queensland Government, 2014). There are 4 major components of IT risk management which is risk identification, risk analysis, risk-reducing measures and risk monitoring (Kakoli, Peter, and Kathleen 1999).

## 2.3 Enterprise Level Information Technology Risk Management

Information system has spread across borders in business environment improves the firms effectiveness and efficiency to maintain the competitiveness and seek ways to improve performance(Anand, 2013). IT derives much of its usefulness from the ability to link systems together to improve functionality and communications and there is no doubt that information technology (IT) or information system (IS) improves the efficiency and efficacy of organization as well as our daily lives. (Ahlan & Arshad, 2011).Previously, IT is perceived to have little strategic value as IT takes the role of back-end support system to an organization. Nowadays, this perception has changed primarily due to the potentials that pervasive IT can provide to all aspects of daily profitable organizations, communities or individuals efficiencies and efficacies and ultimately to achieve strategies and objectives. (Ahlan & Arshad, 2011). The main objective of the enterprise level information technology risk management is to be a holistic and structured approach that aligns IT resources, IT infrastructure, key resources, governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and

managing risk and uncertainties the organization faces as the IT risk is no longer of a technical problem and to be managed in silo. Enterprise level information technology risk management is pertinent to ensure the successful of an organization

### 2.3.1 Perspectives on Information Technology (IT) Risks Management

IT Risks is the likelihood of a particular potential vulnerability and negatively impacts the IT assets which is data, software, and hardware, IT services, key business processes or the whole organization in certain circumstances by a given threat-source. There are quantitative and qualitative methods of assessing IT risks.

IT Risks = F (asset, threat, vulnerability)

Mathematically, by assigning values to information, systems, business processes, recovery costs, quantitative risk can be presented as Annualized Loss Expectancy (ALE) which is expected monetary loss that can be expected for an asset due to a risk being realized over a one-year period (Spremic, 2012). Single Loss Expectancy (SLE) is the value of a single loss of the asset which may or may not be the entire asset. This is the impact of the loss. Annualized Rate of Occurrence (ARO) is how often the loss occurs. This is the likelihood or the number of occurrences of the undesired event. Therefore, impact of the organization risk can be measured and quantify.

ALE = SLE * AR

### 2.3.2 The Fundamentals of Enterprise Information Technology Risk Management Model

The Fundamentals of the enterprise information technology (IT) risk management model are the corporate governance, procedures and operation activities (Ernawati, 2012).

Organizations governance policies for managing IT risks are the policies that are mandatory at all organization levels and approved by the highest corporate bodies either Board, executive management. Typical examples are:

I. Defining the risk appetite which commonly represents the organizations rules and policies for IT risk response strategies which include key metrics, Key Risk Indicators.

II. Organization policies for analyzing the impact IT risks may have on the business either quantitative or qualitative measures for conducting a business impact analysis.

III. Accountability for IT control activities and framework for the IT risk reports.

IV. Establishing Audit or IT Governance Committees and other organizations 'bodies' responsible for managing IT risks.

Procedures for managing IT risks on business units level or functional level represent the guidelines, standards and activities which help in implementation of corporate IT governance policies, for example IT security policy or business continuity plan. According to the regulatory requirements and specific area of

interest, this usually means the adoption of world-wide standards or frameworks such as CobiT, ISO 27001, ITIL, SANS, SAS 70. Periodic internal or external IT audits are needed to detect the level of compliance with standards and regulatory frameworks. IT audits are necessary to identify specific IT controls needed after detect the priority risk areas. Organization need to constantly measure the level of their efficiency and to calculate IT risk level on regular basis.

Lastly, operational or technical activities are aim to raise the level of immunity on threats or attacks to IT assets. Access controls, application controls, system controls, change controls, data accuracy controls, integrity controls and business continuity controls are typical examples of operational IT controls.

## 2.4 Information Technology (IT) Risk Management Plan

The process of risk management usually consist four stages which are risk identification, risk analysis, risk response planning and risk monitoring and control (Hillson, 2002). These steps are sometimes iterative and not always taken in sequence. Generally, an organization is necessary to express these steps in terms of activities and methods. Once these activities are identified, it is then possible to assess the risk management practices implemented. Understanding on the probability of a risk occurring determines the effective management of risk, and if it does occur, the next things is to understand how severe the adverse effect of the risk is likely to be. Between these two domains, organizations may determine the response and risk therefore be avoided, transferred, mitigated or accepted. To a greater extend, external or global risk is the risk that falls outside

an organization's control because they arise outside the realm of the organizations' operations (Frame, 2003).

In order to provide a successful protection for information technology, an organization should develop methods and techniques for the control of the IT incidents and for identification of possible risk evaluation methods. An IT Risk Management plan should have following important steps:

I. IT risk identification and classification

II. IT risk assessment

III. IT risk responses strategies planning

IV. Monitoring of IT risks level

### 2.4.1 Information Technology (IT) Risks Identification and Classification

Identification and classification of risk could be the most difficult aspect of process of managing risks. Generally, risks are identified in terms of their relevance to the specific business objectives or impact on business process rather than only a listing of expected negative outcomes. The classification of risk should according to a proposed organizations framework and preparation for their assessment by categorization of causes and triggers to the risk event, the probability of occurrence, evaluation of their possible impact on business and the allocation of the responsibility to the relevant resources for the risks. There are industry standards and common frameworks able to help organizations to identify and classify IT risks. Apart from industry or country specific risk and regulatory

a classic hierarchical risk approach should able to help in understanding where IT risks exist within the organization:

I. Organizational-level IT risks – these risks are vital part of organizational overall risk management policies and associated with corporate and executive management activities. Typical company or corporate level IT risks include various risks associated with setting up and implementing strategies, procedures, governance models and policies. Some of the examples may be strategic risk (IT strategy planning risks), IT-business misalignment risks, reputation risk, loss of business, risks associated with deficient IT policies and procedures, financial risks (IT project failure, IT investments risk), acquisition risks, legal audit risks (risk that financial statements are incorrect, poor internal IT audit practices) and regulatory risks (non-compliance).

II. Process-level IT risks (IT General Risks) –Business processes and environment are highly automated and integrated with efficient IS and IT. Therefore, execution of company's business processes obviously is associated with IT risks. Typical areas of process-level IT risks are change management procedures and associated risks, software development or acquisition risks, access to program and data risks, business continuity and disaster recovery risks, security administration risks, physical and logical security risks, system risks, information management risks and various security risks.