A STUDY OF RISK MANAGEMENT IN IT SYSTEM TOWARDS A BETTER PERFORMANCE IN ORGANIZATION

SU HUI MIN
PB 12038

BACHELOR OF PROJECT MANAGEMENT
WITH HONORS
UNIVERSITI MALAYSIA PAHANG

A STUDY OF RISK MANAEMENT IN IT SYSTEM TOWARDS A BETTER PERFORMANCE IN ORGANIZATION

SU HUI MIN

Thesis submitted in partial fulfilment of the requirements
for the award of degree of
Bachelor of Project Management with Hons

Faculty of Industrial Management
UNIVERSITI MALAYSIA PAHANG

DECEMBER 2015

SUPERVISOR’S DECLARATION

I hereby declare that I have checked this project report and in my opinion this report is satisfactory in terms of scope and quality for the award of the degree of Bachelor of Project Management with Honors.

Signature :
Name of Supervisor : MADAM ZARITH SUFIA BINTI AZLAN
Position : LECTURER
Date :

STUDENT'S DECLARATION

I hereby declare that the work in this report is my own except for the quotations and summaries which have been duly acknowledged. The report has not been accepted for any degree and is not concurrently submitted for award of other degree.

Signature :
Name : SU HUI MIN
ID Number : PB 12038
Date :

DEDICATION

This thesis is dedicated to my parents and friends who support me all the way during this study.

I would like to dedicate this thesis to my supervisor, Madam Zarith Sufia binti Azlan who give me lots of advice and suggestion throughout my study.

ACKNOWLEDGEMENTS

I am thankful and would like to express my sincere gratitude to my supervisor, Madam Zarith Sufia binti Azlan in providing her germinal ideas, invaluable guidance, continuous encouragement and constant support in succeeding this study. Madam Zarith has always impressed me with her professional in whom it relates to this study. I appreciate her advices during the time of my study. She advices me that this study's purpose is not only to fulfil the final year project but also for the future use which may relate to my career.

My sincere thanks also go to all my course mates who share their knowledge with me in writing and conducting my study. There are many obstacles I faced during this study, but I manage to keep this on until I manage to finish the study. This is because of the advices given by precious friends in UMP.

I acknowledge my sincere indebtedness and gratitude to my parents for the love, dream and sacrifice throughout my life. I also acknowledge the time sacrificing by my lover who understands that it is inevitable to make this study possible. It is hard to express out all my appreciation for their devotion, faith and support in my ability to succeed my goals.

ABSTRACT

The risk in IT system may influence the performance of the organization. In this study, it discusses about the type of risks in IT system and the impact of risk management in IT system towards organization. The scope of this study is focusing on a manufacturing company which using IT system for their daily tasks in order to examine the type of risks in IT system and the impact of the risk management in IT system. A questionnaire has been sent to the respondents and interview was conducted to find out the type of risks and impact of risk management in IT system. There was 20 respondents had participant in this research.

ABSTRAK

Risiko dalam sistem IT akan menpengaruhi prestasi organisasi. Dalam kajian ini, ia membincangkan jenis risiko dalam sistem IT dan kesan pengurusan risiko dalam sistem IT terhadap organisasi. Skop kajian ini memberi tumpuan pada industri perkilangan yang menggunakan sistem IT dalam tugasan harian untuk mengenalpastikan jenis risiko dalam sistem IT dan kesan pengurusan risiko dalam sistem IT. Satu tinjauan soal selidik telah dihantar kepada responden dan temuduga telah dijalankan untuk mendapatkan informasi-informasi yang diperlukan. Seramai 20 orang responden terlibat dalam kajian ini.

TABLE OF CONTENTS

CHAPTER 4 DATA ANALYSIS

CHAPTER 5 CONCLUSION AND RECOMMENDATION

APPENDICES

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In this chapter, it will provide the overview of risk management on the information system (IT) in an organisation and discuss about the problem background of the study and the objectives of the research. The problem statement of a good risk management brings a better performance to the organization will be carry out in this chapter. This chapter will propose the research questions, scope of study, significance of study, expected result and operational definition.

1.2 PROBLEM BACKGROUND

Nowadays, risk management has become more importance in many organizations from different industries. Most of the organizations have set up risk management department to overcome the risks or plan the alternative ways to manage the risk that might be exposed to. Managing the risks has become one of the primary objectives of the organizations. Risk has been defined in many ways. Its definition is depends on the situational contexts. Basically, risk can be concluded as potential loss or failure; it will bring the negative impact to the organizations. However, risk can be concluded as a kind of opportunity for the improvement. The higher the chance of loss or profit, the higher the risk involved. In the research of Williams (2004), Van Scoy (1992) cited that risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. We have to neutralise between the negative impact and the potential benefits of the risks. The project will be success if there is successful risk management in the project because it helps the project manager to have a better control over the project future and able to achieve project objectives (Gary & Larson, 2008).

In this digital era, IT is one of the industries that can generate income in our country. IT industry is recognised as a crucial player in supporting local's sustainable development. This is because IT system is used to process all the information in an organization for a better support. As we know, IT system allowed the workers to operate the company efficiently by providing the complete information. All the records of the company's routine activities and financial document can be stored in the IT system. With the guidance of the system, the top management can streamline the operation of the company for finding the causes of the problems and taking the alternative way to solve the problems. Therefore, organization will try to protect their information assets by implementing risk management.

All organizations are exposed to risks which may bring the negative impact to the organizations. The risks which may bring negative impact to organization must be able to overcome in order to support the organization. In the IT security perspective, risk management is the process of understanding and responding to the causes that may lead to failure in the confidentiality, integrity or availability of an information system (Elky, 2006). IT system risk can be concluded as harm to an organization's operating process or a negative impact to the related information in the organization.

An impressive risk management process is a key element of a successful organization especially in the IT system. The primary objective of the risk management in an organization is to ensure the organization able to prevent or control the risk that brings harm to the organization and achieve the organization's mission and vision but not only just for the IT assets. Thus, the risk management would not only carry out by the IT department who operate and manage the IT system, but as an indispensable component in an organization.

1.3 PROBLEM STATEMENT

Risk is the potential harm that may arise from some current process or from some future event (Elky, 2006). The importance of managing the risk in the organization is to protect the organization’s assets. Therefore, it is important to manage risk in systems. Understanding risk is very important because it allow the system owner to protect the security of information system. Due to the limited resources in the organization, the risk can never be reduced to zero. However, to minimum the risk in the organization, the risk management process have to apply in the organization. Hence, it can bring a better performance in the organization. Therefore, in this study, there is needed to understand the type of risks in IT system and the impacts of the risk management in the organization. Besides, it also studies about the influence of the risk management to the performance of the organizations.

1.4 RESEARCH OBJECTIVES

The objectives of this research are as following:

i. To identify the risks in IT system that influence the performance of the organization.
ii. To determine the impacts of risk management in IT system to the organization.

1.5 RESEARCH QUESTIONS

i. What are the risks in IT system that will influence the performance of the organization?
ii. What are the impacts of the risk management in IT system to the organization?

1.6 SCOPE OF STUDY

The scope of study is to determine the type of risks in the IT system that may influence the performance of the organization and the impact of the risks to the organizations. So, in this study, it will be focus on the organizations which use the IT system to operate their daily activities. The research will carry in the industry area in

Johor Bahru, Malaysia. The respondents who have more experience and high knowledgeable are chosen to collect the information.

1.7 SIGNIFICANCE OF STUDY

IT system can be said that is the main component in an organization. Therefore, the organization needs to ensure that the system can be performed well and minimise the risk or manage the risk which can bring a better performance to the organization.

The most significance of this study is to identify the risks in the IT system that may influence the performance of the organization and determine the impact of the risk to the organization. The result of the study can be as a guideline in any organization which using IT system. After this research, the companies will have a better understanding on the risks that will occur in the IT system and its impacts. The researcher believes this study is very helpful to all the companies to develop an effective risk management. This is because the organization management has to identify the risk and its impact to the organization before set up a risk management process.

In this study, the researcher wants to study about the technical risk in the IT system that will influence the performance of organization. This study may help me to know what risk will be occurred in the IT system and how its affect the organization’s performance.

Last but not least, the information in this study may use as a guideline to do a research in the future. Therefore, the result of the study can also help to minimise the impact to the organization and lead to a better performance.

1.8 EXPECTED RESULT

The expected result of this study is to find out more type of risks that will occur in the IT system and the impacts to the organizations. Besides, the researcher expected that can analyse the major risk and the major impact based on the information that had collected.

1.9 OPERATIONAL DEFINITION

1.9.1 Risk

According to the 4th Edition of the PMBOK Guide, project risk is “an uncertain event or the condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost or quality.”

1.9.2 Risk Management

Risk management focuses on the identifying and assessing the risks to the project and managing those risks to minimize the impact on the project. Risk management is not about eliminating risk but about identifying, assessing and managing risk.

1.9.3 IT System

According to McGraw-Hill Dictionary of Scientific and Technical Terms, IT system can define as the collection of technologies that deal specifically with processing, storing and communicating information which include all types of computer and communication systems.

1.9.4 Organizational Performance

According to the Business Dictionary.com, organizational performance is an analysis of a company’s performance as compared to goals and objectives. There are three outcomes for the performance of organization, which are included market performance, financial performance, shareholder value performance and production capacity performance.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter will cover what is risk management, type of risk in the industry, type of risk in the IT system, the impact of the risk in IT system to the organization, and the impact of risk management. In the risk management practices, it will focus on risk response planning. Therefore, this chapter will discuss the risk management that will involve in this study.

2.2 RISK

In the Oxford Dictionaries, “risk” can be referred to a situation involving exposure to danger or the possibility that something unpleasant or unwelcome will happen. This definition emphasise that “risk” as an alternate of probability or chance in relation to an event or its cause. Risk is the term that a barrier to improve company decision making (Dowie, 1999). Its multiple and vague usages persistently harm the separation of the tasks of identifying and evaluating relevant evidence on the one hand, and evoking and processing necessary value judgements on the other. Risk can be related to adversity which means the risks contribute to adverse effects on project performance (Ward and Chapman, 2003). It also means that the sources of the risk are “things that might go wrong” or the threats to the project.

“Risk” can be referred to uncertain environmental variables that reduce the performance forecasting and lack of predictability in the organization may lead to confuse. Another way of defining “risk” is that risk is a problem that has not happened yet (Cervone, 2006). Besides, “risk” refers to both threat and opportunity. This means that risk is an activity that may bring positive impact or negative impact to the project.. Risk may cause by one or more reasons and more than one impact if it is occurred.

The decision maker will consider both threats and opportunities when doing the decision. Opportunities and threats can be threated separately, but they are seldom independent. However, negligence concern of one of it is not allowed. There are many ways are available to minimize or neutralise the potential threats and offer opportunity simultaneously for a better performance in the project. It is seldom advisable to concentrate on reducing the threats without considering the opportunity (Ward and Chapman, 2003).

In the research of Islam & Tedford (2012), Sadgrove (2005) cited that there are many types of risk in an organization including market risks, credit risks, health and safety risks, environmental risks, fire risks, bomb threats, computer risks, theft and fraud, industrial espionage, technical risks, kidnap and ransom, extortion, accidental and criminal risks and others. Therefore, one of the key factors to lead the business success is dealing with the risks appropriately. Many organizations have realised the demands unstable markets present and have started to adapt to this situation. However, risks and opportunities are greater in this unstable market and this is what they call active strategic risk management.

2.3 RISK MANAGEMENT

Project managers use different methods to execute, monitor and control their projects to ensure the project outcomes are aligned with the project plan. Risk management is one of the methods. Effective risk management is the most important management tool for a project manager who can implement to increase the likelihood of project success (Kwak and Stoddard, 2004). Risk management is intentional to control the level of risk and to reduce their effects (Islam and Tedford, 2012). Risk management has play the important role of an organization’s activities which help all the management activities to achieve the organization’s objectives efficiently and directly.

Risk management can be defined as the forecasting tools to ensure the task or project are keeping on track and aware of the risk by prepared with the solution by the ability itself that have been identified. Risk management is able to create value to a project and improve project performance in terms of cost, time and quality (Azizan and Ibrahim, 2015). Risk management can be concluded as the evaluation and response planning to the uncertainty which definitely be occurred in a project. Risk management is the systematic process of identifying, analysing, and mitigating to the potential project risk. It will maximise the chance of positive impacts and minimise the negative consequences to the project objectives (Adnan, 2009). Risk management is an approach that handling risks after evaluate and analysis to minimise the negative impacts.

Risk management involves procedures, resources and other factors to fulfil safety and other program which lead to reduction of risk level (Islam and Tedford, 2012). Risk management emphasizes on the proactive measures which provide contingency plan to bring the achievement of the project objectives. Smallman & Smith （1999）cited in the research of Azizan & Ibrahim （2015）, risk becomes a complex and topical process that is always misunderstood within the organization and the responsibility of management is unclear. Therefore, a successful risk management is not only depends on the experience of senior managers but the participation of team members are very important. The active participation of employees in the risk management process can ensure the implementation successfully. This is because the employees are important for identifying personnel and work environment related risks (Close, 1974).

The range of risks faced by businesses and their projects today is huge and arising from multiple of sources which including the internal and external factors such as technical, management, operational and commercial issues (Hillson, 2003). Some risks may cause by changing in condition or scope of work, inappropriate assumptions, use of new technology and methods. The practice of risk management has a tendency to be focused on the threats rather than the opportunity (Pons, 2010).

2.3.1 Practices of Risk Management

Risk management is an on-going process throughout the project life cycle. The risk management process can be divided into two interrelated phases, which are risk assessment and risk control. Then, these two phases are further broken down. According to the research of Williams (2004), Boehm (1989) had mentioned that risk assessment involves risk identification, risk analysis and risk prioritization. On the other side, risk control involves risk planning, risk mitigation and risk monitoring. All of these processes will be updated as the new risks may occur throughout the project life cycle. Therefore, risk management is to reduce the probability and negative impacts of those risks.

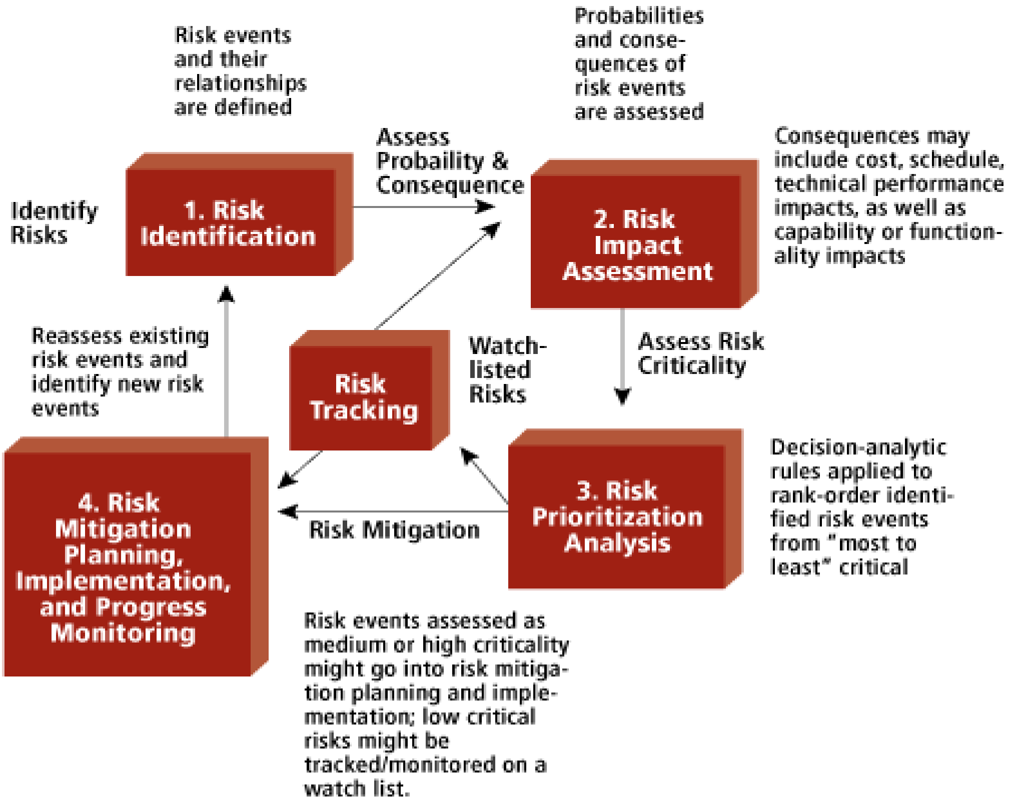
Risk events and their relationships are defined
Probabilities and consequences of risk events are assessed
Identify Risks
1. Risk Identification
Assess Probaility & Consequence
2. Risk Impact Assessment
Consequences may include cost, schedule, technical performance impacts, as well as capability or functionality impacts
Reassess existing risk events and identify new risk events
Risk Tracking
Watch-listed Risks
Assess Risk Criticality
4. Risk Mitigation Planning, Implementation, and Progress Monitoring
Risk Mitigation
3. Risk Prioritization Analysis
Decision-analytic rules applied to rank-order identified risk events from "most to least" critical
Risk events assessed as medium or high criticality might go into risk mitigation planning and implementation; low critical risks might be tracked/monitored on a watch list.

Figure 2.1: Risk management practice (The MITRE Corporation, 2015)

The Figure 2.1 show the risk management practice in a project life cycle. Usually, the risk management practice involved risk identification, risk impact assessment, risk prioritization analysis and risk mitigation, planning implementation and monitoring process.

2.3.1.1 Risk Identification

The risk identification starts at the beginning of the project. The number of risks will increase as the project keeps going through the lifecycle. As the nature of the projects, especially at the initial stages, the high-risk decisions must be made and the resources for a project need to be allocated to ensure the project was carried on and do not delay the schedule of the project. Hence, project managers need to spend a lot of time and effort to assure the decision are made wisely, so that the product or process does not have to be redesigned at later stage (Patterson et al., 1999). Thus, risk identification stage can be considered as one of the most important stages within the risk management practices. However, the project must been initiated before the risk identification can take place. The management and team members should fully committed to the process and developed the project planning information such as work breakdown structure (WBS), the risk identification can the take place. When a risk is being identified, it need to assess to ascertain the probability of occurring of impact to the schedule, cost and quality, and then prioritised. The PMBoK (Project Management Institute, 2008) had suggested several methods for risk identification such as specific questionnaires or checklists, brainstorming sessions, interviewing experts and so on. Based on the result of the research of Islam & Tedford (2012), around 48% of respondents agreed to use the historical data for similar projects to identify the risk occurred to their selected Design and Build.

2.3.1.2 Risk Analysis

The risk analysis will be carried out right after the risks have been identified and enumerated. The risks that were identified can be used for decision-making information. This means that each risk is considered about the probability and the seriousness of the risk. Risk analysis can identify the likelihood the risks that have been identified will occur. Risk analysis can present in a risk diagram.

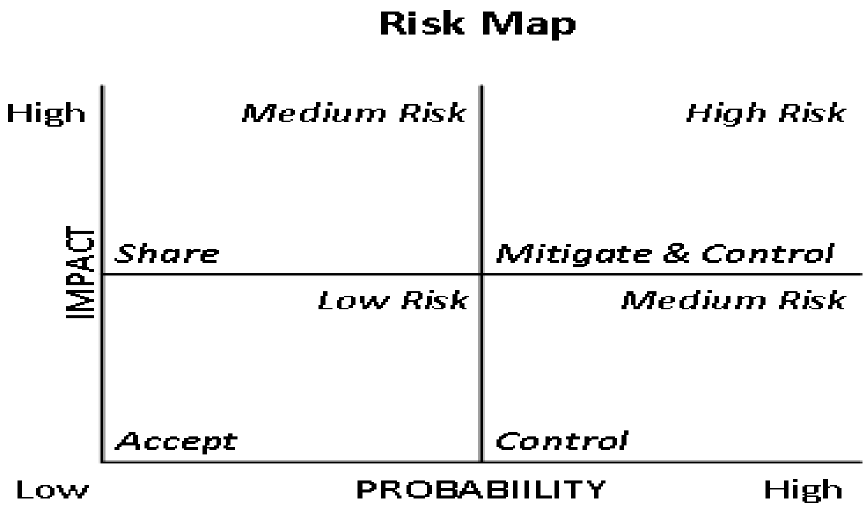

Figure 2.2: Risk diagram (Vancouver Island University, 2015).

The risk diagram (Figure 2.2) shows an overall view upon all risks and put more attention to the most important risks. Besides, the risk diagram illustrates that whether the risks can be reduced by decreasing the probability or the impact.

2.3.1.3 Risk Prioritization

After the risks have been managed into a risk diagram, then it can prioritise the risks by ranking them. This is because it is a waste if taking the unnecessary action to every identified risk. Moreover, every project has only got the limited resources. Some of the identified risks may have a very low impact or very low probability of occurring. Prioritisation of risks has to be grounded on reliable expert knowledge and available historical data to allow an accurate estimation of probabilities and level of impacts of the risks to the organizations (Baccarini and Archer, 2001). Through the process of prioritization, the management can determine which risks need to take the action on. The management can sort the list from high probability and high impact risks to low probability and low impact. The management may use the categorical values to rank the risk. For example, they can categorise the probability of risks into very improbable, improbable, probable or frequent; or the impact of risks into negligible, marginal, critical or catastrophic.

According to the Cervone (2006), there is a more stable measure of risk prioritization can be achieved by combining the elements of strategies from several matrix-based schemed. Cervone had mentioned that this combination was evaluating the risks from three dimensions, which are impact, probability and discrimination. The effect of this ranking model is similar to the proposed by Traeger (2005) which cited in the research of Cervone (2006). The first dimension, impact, is taken directly from the research of Lansdowne (1999). Cervone mentioned that Lansdowne used a five-point scale for evaluating risk impact.

i. Critical risk (5 points) – would cause the project failure.
ii. Serious risk (4 points) – would cause major cost or schedule increase and requirement may not be achieved.
iii. Moderate risk (3 points) – would cause moderate cost or schedule increase but the main requirement still can be met.
iv. Minor risk (2 points) – would cause only small cost or schedule increase.
v. Negligible risk (1 point) – would have no substantive effect on cost or schedule.

The second dimension, probability, is taken from the research of Cervone (2006) which cited by Kendrick (2003).

i. High probability (5 points) – likely occurrence.
ii. Medium probability (3 points) – unlikely occurrence.
iii. Low probability (1 point) – very unlikely occurrence.

The third dimension, discrimination, is based on the criteria from Kendrick (2003) which provide an additional perspective that is designed to estimate the impact of risk to the overall framework of the project.

i. High effect (1 point) – project objectives are at risk which will result a change to scope, schedule and resources.
ii. Medium effect (3 points) – project objectives will be achieved but replanning is required.

iii. Low effort (5 points) – no major plan changes will result.

Therefore, after the risks are evaluated by three dimensions, a point value can be assigned to each risk using the formula:

Overall risk factor = (Probability*Impact)/ Discrimination

Hence, all the project risk factors can be ranked by severity of risk and overall potential impact to the project (Cervone, 2006).

2.3.1.4 Risk Response Planning

Risk response planning should be developed for each of the "above the line" prioritised risks. So, the proactive action can take place (Williams, 2004). According to PMI (2013), risk response planning is the process of developing options and determining actions to enhance opportunities and reduce the threats to the project objectives. There are four different response types:

i. Avoid

According to (Seifert, 2014), avoid here means an identified risk is no longer relevant due to changes in project plans. For example, this response planning action can take place through information buying. Investigation can obtain more information to reduce the risk.

ii. Transfer

Another type is transfer which means the risks are transferred to third party through contract or insurance. The organization can cover any financial loss occurred by purchasing an insurance.

iii. Mitigate

Then, the mitigation is the probability and the impact of a risk can be reduced through prevention. Risk mitigation produces a situation in which the risk items are eliminated or otherwise resolved.

iv. Accept

Last but not least, accept means that there is no action is taken although negative impacts have been noticed while a conscious risk is occurring. In the research of Williams (2004), he cited that Hall (1998) said sometimes the organization consciously chooses to live with the consequences of the risk and the results of the potential loss.

2.3.1.5 Risk Mitigation

For every identified risk, an action must be implemented. The project team has the responsibility to select a suitable risk response for each risk. The level of actions to mitigate the risk is determined by the probability of the risk and the impacts. Risk mitigation is the most common considered risk management strategy. Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw (Elky, 2006). Sometimes the determination of mitigation strategies process is called control analysis. The responsible of senior management become more important to use the lowest cost approach with minimum adverse impact to the organization as the elimination of all risks is close to impossible. The goals and mission of an organization should be considered in selecting any of risk mitigation options (Stoneburner et al., 2002). The priority should be given to the risks that have higher potential impact to the organization. Besides, each organization has different environment and objectives, so the method of mitigate the risk may vary.

2.3.1.6 Risk Monitoring

As the project proceeds and the organizations' environment are not static, the risk status might be changed. New risks will materialise and others will be reduced or solved. Therefore, it is compulsory for the management to monitor the progress of the product and the resolution of the risk items when the risks are identified, analysed, prioritised, and actions are established. Therefore, the project team can take the corrective action if necessary. The monitoring is an on-going process throughout the whole project via risk management activities. Risks need to be monitored regularly to determine whether its probability and impact change if there is new circumstances occur. A key to successful risk management is that proactive actions are owned by individuals and are monitored (Larman, 2004).

2.4 INFORMATION TECHNOLOGY (IT) SYSTEM

Information technology (IT) system plays an important role in any organization's business. IT system is at the core of information management of the organization and allows it to operate efficiently and maintain its competitive advantage (Adeleye et al., 2004). Adeleye, Annansingh, & Nunes (2004) mentioned that O'Brien (1996) said "if information systems do not properly support the strategic objectives, business operations, or management needs of an enterprise, they can seriously damage its prospects for survival and success". Then, it was proposed by Drucker (1996) in the research of Adeleye et al (2004), in today's knowledge-based society, information is the framework around which organizations are formed. As we know, IT system can provide a better data distribution, complete business processes and network communications to enable a better customer relationship. Today's information system must truly add value to the organization through the creation, capture, distribution, application, and leveraging of knowledge (Bolney, 1999).

IT systems provide a better data, quicker data access or more favourable solutions in order to assist the managers and other decision-makers. The managers used the IT systems to help them complete the task more efficiently and gather the information. Broady-Preston and Hayward (2001) stated that in the current turbulent business environment, quality information is required to ensure the organizations to achieve competitive advantages by using such information to make decisions more rapidly than their rivals. In this competitive economic business condition, every organization must exploit information effectively to ensure better performance in the market. In the Broady-Preston and Hayward's research, cited that the Library and Information Commission (1998) noted information is an international commodity and knowledge underpins all successful economic activity.

In this modern generation, organizations need to have a perpetual strategy process to ensure their organizations have the competitive advantage. The organizations must take the advantages of technology so they will not be out dated. However, simply storing and recovering information is not enough for the information advantage. The organizations have to match the information to their strategic processes. Broady-Preston and Hayward mentioned that Frappaolo (1998) cited organizations are increasingly measuring the value of their information assets on the basis of their ability to utilise such assets to response to market demands more effectively than their competitors.

2.5 RISKS IN IT SYSTEM

Risk is a part of all aspects of everyday life. Risk is an uncertainty event which may bring negative impact to the project by considering its probability and impact. Development of an IT system is a complex process which makes it submissive to a great number of risks (Đurković and Raković, 2009). IT managers can balance the operational and economic costs in protecting the IT systems and the data which support their organizations' objectives by using risk management process. This process pervades decision-making in all areas of our daily lives. Many projects do not achieve the objectives because the ignorance of the development of informational system.

2.5.1 Threat

A threat is the potential for a particular threat source to successfully exercise a particular vulnerability (Stoneburner et al., 2002). Vulnerability is a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised. The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. A threat source is any potential activity to cause harm to an IT system. It is important to consider the entire potential threat sources that could cause harm to IT system, so the threat statement which list down the threat source can be evaluated.

The common threat sources are:

1. Natural threat
2. Human threat
3. Environmental threat
4. Technical threat

2.5.1.1 Natural Threat

Natural threat can best be thought as threat caused by Mother Nature such as earthquakes, floods and tsunami. These natural disasters may cause the damage or destructions of system hardware or software assets and lead to partial or total outage. For example, an internal or external fire may cause damage to hardware of the computer system and facility. The internal or external flooding may cause the destruction of system hardware. Earthquakes are among the most deadly and destructive of natural hazards. It often destroys power and telephone lines.

Secondary disaster can be concluded as natural disaster. Secondary disasters are usually resulting from natural disasters or environmental conditions. The secondary disasters can strike communities at any time. For example, broken water pipe could result in internal flooding. Spilled chemicals could cause a fire. A structural fire which caused by fire may lead to power failure by burning out the circuits.

2.5.1.2 Human Threat

Human threat is the activities that are normally caused by human beings such as unintentional acts or deliberate actions. A deliberate attack can be either a malicious attempt to gain unauthorized access to an IT system in order to compromise system and data integrity or attack with nonetheless purposeful, attempt to circumvent system security.

Data entry errors or omissions are a human threat in IT system. Data entry errors and omissions are mistakes in keying or oversight to key data. This could affect system resources and the safeguards that protecting other system resources. For example, an unauthorised success to a sensitive data if the unnecessary accounts such as guest accounts and employees that no longer need access to system were failed to delete or disable. Incorrect values were entered for sensitive information such as financial data or personally information could lead to data inconsistency.

Espionage is another human threat to IT system. Espionage can bring the significant impacts to the data confidentiality. If it combines with other threats, they could affect data integrity and availability. Espionage is an act of spying to obtain important information through copying, reproducing, recording and photographing. Foreign government may conduct espionage through the electronic bugs. Sometimes, foreign government may put an employee into the target organization by either bribing or blackmailing the employee. The licensing and on-site liaison officers can provide unauthorised chances to collect the information during the legitimate business agreements.

Inadvertent acts or carelessness could impact data confidentially, integrity and availability. Most of the system performance demeaning or loss of system are caused by the unintentional act of human. Software vulnerabilities such as programming and development errors could lead to loss of data confidentiality after they are compromise. Data errors such as entry, deletion and corruption errors are usually caused by the incorrect operations of synchronizing databases. Flaw of data could lead to loss of data confidentiality which caused by improper upgrades of database management software. Installation, upgrade and maintenance errors may leave data unprotected or overly exposed to security vulnerabilities. The unauthorised access to system and data can be prevented by terminated the employees' card keys.

Terrorism is an individual or a group who take the violent act to sabotage the condition or infrastructure especially aim for the political and social sentiment. For example, the terrorism attacked on September 11, 2001. The terrorism in IT system refers to cyber terrorism or information warfare. For example, according to the New York Times News Service in August 1996, the U.S. Justice Department's website was shut down after members of public called to report that the site had been altered, apparently by a hacker or hackers who post nude photographs and attack on the Communication Decency Act. A department spokesman, Joe Krovisky said that the hacker replace information on the home page with obscenities, graffiti and anti-government statements.

Damage or loss of system assets can be resulted from the theft, sabotage and vandalism. These acts could also lead to other risks like interconnected system's damage. For example, dissatisfied employees will try to damage the system to release their angriness. They can install some software to destroy a computer system. Logic bombs could destroy system data at a given time or under certain circumstances. Some of these sabotage action may destroy the data which might not be recovered. System assets' loss can be caused by those intentional or improper use and computer abuse.

2.5.1.3 Environmental Threat

Electromagnetic Interference (EMI) is the result of signal transmitters and receivers operating to a content management system (CMS) which will lead to the integrity and availability of the system. It will cause an interruption in the system of electronic operation. One of the examples is malfunctioning equipment. Line noise which caused by electromagnetic impulses and radio frequency interference could affect the corrupted data transfers. For example, data transfer from CPU to disk, printing errors, power supply damage and static on computer monitor screens. The contents of the computer screen can be reconstructed by electromagnetic radiation. If these signals contact with the exposed cables or telephone lines, it can carry a several hundred feet of distance.

The controlled and non-controlled environment conditions have the potential to affect the damage of the system. The natural environment such as extremely high or low in temperature, humidity, and poor design of ventilation and air conditioning system. Overheating in computer rooms may cause the computer operation failure and downtime. Besides, both excess and insufficient humidity in the computer room could threaten system reliability. If the water leaks into the server rooms, it will cause the equipment damage.

Hazardous material accident such as unintentional scatter of toxic liquid could cause the system availability especially the substances that are flammable, combustible, explosive, toxic, noxious, corrosive or radioactive. The office cleaning materials may content combustible materials which can cause the explosion if spilled or do not keep at a specific temperature. The extremely corrosive chemical drain cleaners include lye or sulphuric acid which would eat away materials including skin if there is a contact. Therefore, if these chemical contacts with the computer hardware may cause the system break down and unable to function.

An intentional or unintentional act of physical cable cut may affect the ability of system to perform its intended function. The effect of the system can be ranged from minimal to catastrophic by considering the power and communications backups which built into the system. The example of unintentional event is lightning strikes can cause a structural fire which could burn out circuits resulting in a power failure. The other example for intentional event is disgruntled employee may sabotage transmission media.

Insufficient or excessive power may cause by the disruption in the primary power source or power fluctuation such as power spike or blackout. The timeliness and delivered service's quality will be affected by power outage and malfunction or failure of CPU or hardware.

2.5.1.4 Technical Threat

There are several types of technical threat that will cause harm to the IT system. System operation can easily affect by corruption of system or system errors. Database failure which result of system software or hardware's failure could lead to financial loss of the company. Some of the tasks could not be carried on as a result of failure in application software except for those could be done manually. The system might be placed in a risk condition if the weakness is newly discovered and not addressed by requirements.

The intentional violation of data integrity might be caused by data or system contamination which is mixed data in different sensitivity levels. The unauthorised person might disclose to the data values which stray from their field description and business rules. The input into dynamically generated web pages such as malicious tagging could lead to cross-site scripting attacks (CSS). An attacker can destroy the data integrity, set and read cookies, intercept user input and execute malicious scripts by client in the context of the trusted source by using malicious tagging. For example, Citibank closed a CSS vulnerability identified by De Vitry at the bank's C2IT.com Internet payment site that enabled attackers to grab users' credit card and bank account information.

Eavesdropping is the intentional act to get the protected information from others. The people may misuse the protected information to get the other information. The eavesdropping devices can be used to intercept sensitive and unencrypted data such as electronic bugs. For example, all the user input can be reproduced by using keystroke monitoring. Use of Packet Sniffers can permit unauthorised intercept of transmission. These transmissions can include sensitive information such as passwords over networks. User or system activities can be captured by using Trojan Horse applications.

The summary of the risk in IT system is show in Table 2.1 as below.

Table 2.1: Summary of risk in IT system

	THREATS
Natural threats	i. Natural disaster ii. Secondary disaster
Human threats	i. Data entry errors or omissions ii. Espionage iii. Inadvertent acts or carelessness iv. Terrorism v. Theft, sabotage, vandalism or physical intrusions
Environmental threats	i. Electromagnetic Interference (EMI) ii. Environmental conditions iii. Hazardous material accident iv. Physical cable cuts v. Power Fluctuation
Technical threats	i. Corruption by system, system errors or failures ii. Data or system contamination iii. Eavesdropping

2.6 IMPACT OF RISK MANAGEMENT IN IT SYSTEM

People nowadays are given great abilities to process, store and transmit digital data in their business field in this rapid evolution of electronic networks and computer based information system. This had made changes in communication and information technologies and raised the awareness of protection of organization's information assets. The entities, companies and organizations have assets of a material or immaterial nature that may damage which lead to the risks occurred. Facing pressure of organizational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understand the security concerns (Dhillon and Backhouse, 2000). The adverse impact of risk in IT system can be described in terms of loss or degradation or combination of the following:

i. Integrity
ii. Availability
iii. Confidentiality
iv. Tangible impacts

Information system security will not only address to the data but the organizational context which always been used. The traditional information security principles of confidentiality, integrity and availability are fine as far as they go, but they are very restricted. They apply most obviously to information seen as "data" held on computer systems.

2.6.1 Data Integrity

System and data integrity refers to the requirement that information be protected from improper modification. Integrity refers to maintaining the values of data stored and manipulated, such as maintaining the correct signs and symbols. If there are any unauthorised changes to the data or IT system, the integrity can be concluded as lost. It could result in inaccuracy and wrong decision making if the data integrity is not corrected and continued use by the management.

Employees who can interpret the symbols processed and stored but not only to the numerical and language skills are needed in the business sectors. The employees need to have the ability to use the data in a way that accords with the prevailing norms of the organization. One of the examples is checking the creditworthiness of a prospective loan applicant. This process requires both data on the applicant and correct interpretation according to company rules. A secure organization must able to interpret the data but only to secure the data.

2.6.2 Confidentiality of Data

System and data confidentiality is the protection of information from unauthorised disclosure. The impact of unauthorised disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Loss of public confidence, embarrassment, or legal action against the organization may result from unauthorised, unanticipated or unintentional disclosure.

2.6.3 Availability of Data

Availability is the condition that the systems are available to use when the organization need it. The organization’s mission is affected when a mission-critical IT system is not available to the end users. System failure is an organizational security issue. It could lead to loss of productive time and hinder the end users’ performance of their functions in supporting the mission of organization if the functionality of the system is lost. Therefore, this problem can be improved by implementing risk management in IT system.

2.6.4 Tangible Impact

2.6.4.1 Simplified Report Building and Analytics

The management reports are required a lot of time and effort to finish especially the data is using in several databases at the same time. It will increase the probability of error occurred when the data is standardised into the common format which set by the organization. Besides, the data in multiple currencies and different languages will increase the complicatedness of the task. After the extraction and standardisation is completed, the report can finally be built. In addition, when the report is needed, this whole process has to be repeated every time.

Therefore, these challenges largely go away by implementation of risk management in IT system as data is standardised into common format, currency and language. At a press of button, a report can be automatically generated in a short time. Moreover, the employees can filter the data by using extensive range of criteria. There are more time to spend for analysing the information, spotting trends and correlations, making decisions and apportioning resources to manage the risk given to the risk manager and the team.

2.6.4.2 Better Operational Efficiency

Employees can effectively performing the same manual quality checks and maintenance for their data by using multiple systems and databases. Therefore, everyone can enter into the same online system simultaneously at any time to get the data they want by implementing the risk management in IT system. The organization has a consistent process for the data collection. The communication of the system can make any changes of the data. Data loads or direct feeds can integrate the data which held in other systems and by third parties automatically.

2.7 THEORETICAL FRAMEWORK

The relationship between independent variable and dependent variable is summarised into a form of theoretical framework as stated below:

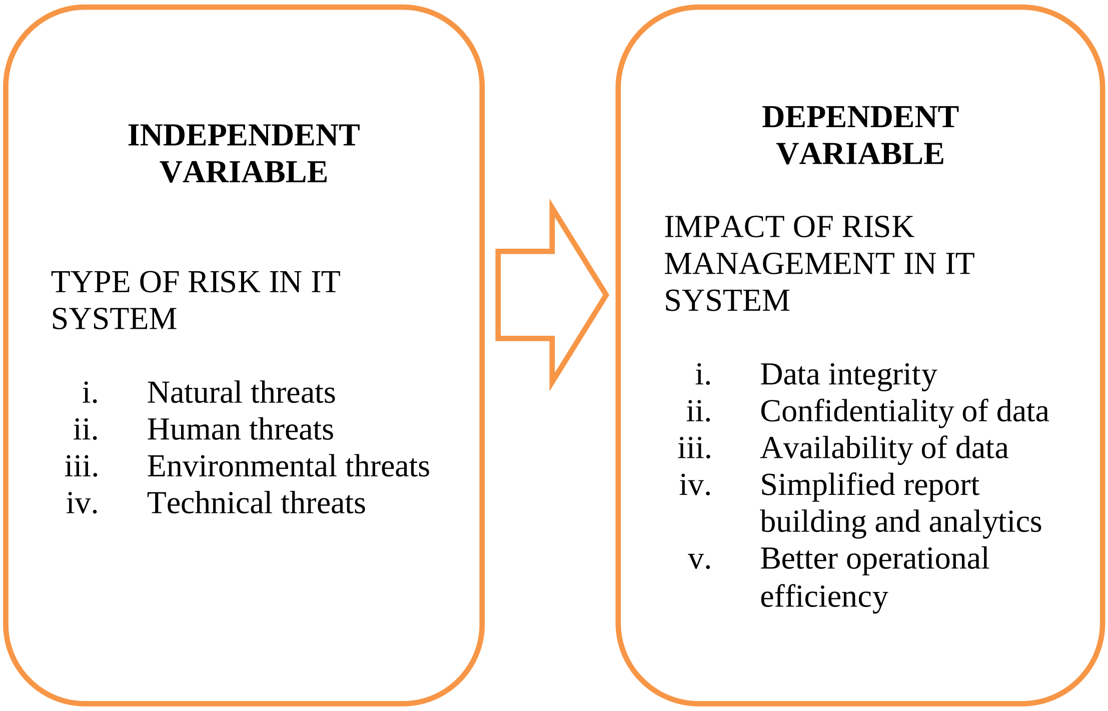
INDEPENDENT VARIABLE
TYPE OF RISK IN IT SYSTEM
i. Natural threats
ii. Human threats
iii. Environmental threats
iv. Technical threats
DEPENDENT VARIABLE
IMPACT OF RISK MANAGEMENT IN IT SYSTEM
i. Data integrity
ii. Confidentiality of data
iii. Availability of data
iv. Simplified report building and analytics
v. Better operational efficiency

Figure 2.3: Theoretical frameworks of type of risk and the impact of risk management.

2.8 REVIEW OF RESEARCH METHODOLOGY OF SIMILAR RESEARCH

Previous studies that have been carried out by the researchers on risk management in IT systems in terms of subject matter and research methodologies are show in the Table 2.2 as below.

Table 2.2: Previous researches on risk management in IT systems

NO	AUTHOR	YEAR	PLACE OF RESEARCH	NAME OF ARTICLE/JOURNAL	RESEARCH AREA	METHODOLOGY	RESPONDENTS
1	Bunmi Cynthia Adeleye, Fenio Annansingh, Miguel Baptista Nunes	2004	Nigeria	Risk management practices in IS outsourcing: an investigation into commercial banks in Nigeria	Risk management practices	Questionnaire	From 15 commercial banks
2	Gary Stoneburner, Alice Goguen, Alexis Feringa	2002	U.S.	Risk Management Guide for Information Technology Systems	Overview of risk management in IT systems	Literature review	-

3	Steve Elky	2006	U.S.	An Introduction to Information System Risk Management	IT risk assessment	Literature review	-
4	Ozren Đurković, Lazar Raković	2009	-	Risks in Information Systems Development Projects	Risk management methodology	Literature review	-
5	Božo Nikolić, Ljiljana Ružić-Dimitrijević	2009	Serbia	Risk Assessment of Information Technology Systems	Methodology of risk management in IT area	Literature review	-
6	Bouchaib Bahli, Suzanne Rivard	2001	Canada	An Assessment of Information Technology Outsourcing Risk	Risk management of IS outsourcing.	Questionnaire survey	390 respondents from Senior IS Executive
7	Claude Sicotte, Guy Pare, Marie-Pierre Moreault, Andre Paccioni	2006	Canada	A Risk Assessment of Two Inter-organizational Clinical Information Systems	Risk analysis framework	Case study	2 respondents from Inter-organizational Clinical IS

2.9 CONCLUSION

Risk is a factor that cannot be prevented in information technology system. Therefore, it is very important to take it into consideration in an organization. Risk management should play an important role in managing IT system to ensure the organization’s operation is conduct smoothly. It is necessary to determine some methodologies of risk management in order to identify all the risk in the IT system. Then, a risk responding plan should be carried out to mitigate the risk in the system. Last but not least, monitoring is another important part after the risk responding plan is carried out, as well as periodically identifying and examining again the current and new risks which can threat the IT system in the organizations.

CHAPTER 3

RESEARCH METHOGOLOGY

3.1 INTRODUCTION

In this chapter, the research will discuss more information about the research methodology that used in this study. Several information that will be covered in this chapter which included research design, research method, population and sampling, data collection technique, design of questionnaire and data analysis.

3.2 RESEARCH DESIGN

A research design is not just a work plan. A research design contains the details what has to be done to complete the project. The function of a research design is to ensure that the evidence obtained enables the researchers to answer the initial question as unambiguously as possible (De Vaus and de Vaus, 2001). Obtaining relevant evidence indicates specifying the type of evidence needed to answer the research question, to test a theory, to evaluate a programme or to accurately describe some phenomenon. There are three fundamental types of researches:

i. Descriptive research
ii. Exploratory research
iii. Causal research

Descriptive research is conducted to determine and be able to describe the characteristics of variables of interest in a situation. Descriptive research encloses much government sponsored research including the population census, the collection of a wide range of social indicators and economic information (De Vaus and de Vaus, 2001). Descriptive research is divided by three types of method which are observational method, survey method and case study method. Observational method sometimes refers to field observation. In survey method, respondents answer the questions through interview or questionnaires. After that, researchers will describe the responses given. Case study research involves an in-depth study of an individual or groups. Case study often leads to testable hypothesis and allow the researchers to study rare phenomena. In addition, descriptive research can be either quantitative or qualitative. Quantitative research is asking people for their opinions in a structured way, so the researchers can produce the hard facts and statistics in the research. Quantitative research involves a large number of respondents who are in the target communities. On the other side, qualitative research is the information that gets from the respondents which are not in numerical form.

Exploratory research is not only helps people to have a better understanding of the problems, but it provide conclusive evidence. Exploratory research does not aim to provide the final and conclusive answers to the research questions, but explores the research topic with varying levels of depth. In Research-methodology.net (2015), there mention that Brown (2006) cited exploratory research tends to tackle new problems on which little or no previous research has been done. Singh (2007) who mentioned in the Research-methodology.net (2015) noted that exploratory research is the initial research, which forms the basis of more conclusive research. It can even help in determining the research design, sampling methodology and data collection method.

Causal research is usually conducted to identify the extent and nature of cause-and-effect relationships. It can be conducted to assess impacts of specific changed on existing norms, various processes and so on.

3.3 RESEARCH METHOD

Descriptive method will be using in this research. As mentioned in the previous subtopic, there are three main types of researches which are observational method, case study method and survey method. In this research, case study method will be using and respondents will answer the questions through questionnaire. In this research, the type of risks in IT system and the impact of the risk management will be carrying out.

3.4 POPULATION AND SAMPLING

According to Sekaran et al (2010), population refers to the entire group of people, events or thing of interest that the researcher wishes to investigate. The population of this research will target on two organizations within the state of Johor Bahru, Johor which using IT system to operate their routine activities in the organizations.

Sampling is the process of selecting a sufficient number of elements from the populations (Sekaran et al, 2010). Sampling is divided into two types which are probability sampling and nonprobability sampling. Probability sampling consists of unrestricted sampling and restricted sampling. On the other hand, nonprobability sampling includes convenience sampling, volunteer sampling, judgement sampling and quota sampling.

In this study, the sampling method that will be used is judgement sample. Judgement sample is the data selected based on opinion of one or more expert person. Random sampling will be using in this research. 20 samples are randomly selected from a company in Johor Bahru which established for 10 years to complete the questionnaire.

3.5 DATA COLLECTION TECHNIQUE

Data collection is the process of collecting data to be processed and analysed in order to achieve certain objectives. This topic explains how the data will be collected and what are the methods or techniques are used to collect data.

At the beginning of data collection, the questionnaire was distributed to the targeted sample through email and fax. This method frequently used because questionnaire can be able to collect data in more short time with lower cost. Other data collection technique might more expensive and timely compare to the questionnaire method. After email and fax to questionnaire to the company, a phone call is made by the researcher to request the respondents to fill the questionnaire for data collection purpose and doing interview.

A cover letter will be attached with the questionnaire (refer Appendix A). The cover letter is explained the purpose of questionnaire and parts of the research questionnaire. The deadline will be given to the respondents to complete the questionnaire.

3.6 DESIGN OF QUESTIONNAIRE

Questionnaire is used to collect the data. This questionnaire contain open ended and close ended question. The relevant info is filled in the open ended question whereas the questionnaire was scaled in the close ended question. This questionnaire consists of three sections.

Section A: Demographic of respondent
Section B: The type of risk in IT system
Section C: The impact of risk management in IT system to organization

Section A is to obtain and understanding more about the company respondent profile. It includes general questions which included the personal information of respondents such as their name, working department in the company, experience, age, gender and educational level. The respondent is requested to fill in the relevant information in this section A questions.

Section B includes the list of type of risk in IT system. This section will ask about how frequently of the risk in IT system occurred in the company. This section included ranking question and open ended question. The respondents can give their opinions about the other type of risk in IT system. The types of risk in IT system are categorised into four groups which are as follow:

i. Natural threats

ii. Human threats
iii. Environmental threats
iv. Technical threats

Section C will focus on the impact of risk management in IT system to an organization. This section will contain open ended and close ended question. There are five groups of impact of risk management in IT system to organization which are:

i. Data integrity
ii. Confidentiality of data
iii. Availability of data
iv. Simplified report building and analytics
v. Better operational efficiency

In addition, the respondents requested to give their opinion in how to increase the impact of risk management in IT system to the company through an open ended question at the end of the questionnaire. Many researchers like to use Likert-type scale because it is easy to analyse statistically. A five point scale will be used in Section B and C. In Section B, the question is ranging from the never (1) to the almost always (5). In Section C, the question is ranging from the strongly disagree (1) to the strongly agree (5).

3.7 DATA ANALYSIS

Data analysis will be conducted after all the data was collected to determine the result of the study. The data from questionnaire are analysed using Microsoft Excel 2010 because it is familiar and the analysis is visible in Microsoft Excel 2010. The researcher used the simplest method to analyse the data which is descriptive statistics method. Descriptive statistics are the raw data is transformed into the information to describe a set of factors in a situation. Descriptive statistics are provided by frequencies and measures to obtain the respondents’ demographic profile.

3.8 CONCLUSION

In this study, the methodology was planned to achieve the objectives. Therefore, the main purpose of the data collection is to achieve the research objectives and answered all question in this study. This chapter explained in detail about research design, questionnaire design, population and sampling and data collection method.

CHAPTER 4

DATA ANALYSIS

4.1 INTRODUCTION

This chapter shows the results of the research data analysis by using Microsoft Excel. The findings are presented accordingly included demographic characteristics of the research sample, followed by the results of the interview. The result of the data were presented in table, so that more clearly and easy to understand.

4.2 DEMOGRAPHIC ANALYSIS

In this study, demographic analysis is to determine the frequency, mean and mode of respondent's background, which included age, gender, working experience, working department in company and the level of education.

In this research, 20 questionnaires were successfully distributed by using email to a company in Johor Bahru. 20 completed questionnaires were managed collected, which yield a response rate of 100%. Interview had been conducted in that company to get a deeper opinion from them. The interviews are kept on until all the requirements of this research are collected. The company will be selected as it has 10 years' experience in the manufacturing industry. The amount of employees is around 280 people.

4.2.1 Age

The age of the respondents is being analysed and the distribution of age among respondents were shown in the Table 4.1. There were 4 respondents (20%) who were under the categories of 25-29 years old, 5 respondents (25%) who were under the categories of 30-34 years old, 3 respondents (15%) who were under the categories of 35-39 years old, 5 respondents (25%) who were under the categories of 40-44 years old and lastly, there were 3 respondents (15%) who were under the categories of 45-49 years old.

Table 4.1: Frequencies of age

Age	Frequency	Percentage (%)
25-29	4	20
30-34	5	25
35-39	3	15
40-44	5	25
45-49	3	15
	20	100

4.2.2 Gender

Table 4.2 shows the gender's percentage of the 20 respondents who involve in this survey. From the total number, female respondents achieve higher percentage compare to male respondents, which is 60% (12 people) whereas male respondents were just achieved 40% (8 people).

Table 4.2: Gender of respondents

Gender	Frequency	Percentage (%)
Male	8	40
Female	12	60
	20	100

4.2.3 Working Experiences

Table 4.3 shows the working experiences of the respondents in the company. Majority of the respondents have 6 to 10 years of experience in this field, which is 40%, 8 out of 20 respondents. Following is the second highest percentage is 1 to 5 years, 25% (5 people). Besides that, the percentage of both 11 to 15 years and more than 20 years are 15% (3 people). Working year range among 16 to 20 years showed the lowest respondent which is only 5% (1 person).

Table 4.3: Working experiences of respondents

Working Experience	Frequency	Percentage (%)
1 to 5 years	5	25
6 to 10 years	8	40
11 to 15 years	3	15
16 to 20 years	1	5
More than 20 years	3	15
	20	100

4.2.4 Working Department in Company

Table 4.4 shows the working department of respondents in the company. According to the table 4.4, the highest frequency of the department is IT department which has 5 people (25%). Following are the second highest percentage is R&D department which contribute 20% (4 people). Warehouse department and Human Resource department have the same percentages which are 15% (3 people). Marketing department and Operation department have the same percentages too which are 10% (2 people). Lastly is the Supply Chain department which is 5% (1 person).

Table 4.4: Working department of respondents in company

Department	Frequency	Percentage (%)
Warehouse	3	15
IT	5	25
Marketing	2	10
R&D	4	20
Human Resource	3	15
Operation	2	10
Supply Chain	1	5
	20	100

4.2.5 Educational Level

Table 4.5 shows the highest education level of respondents in the research. The degree education level achieves highest percentage which is 65%, 13 people out of 20. The second highest percentage is other education level such as diploma which is 25% (5 people). The following is STPM which is 10% (2 people).

Table 4.5: Highest educational level

Educational Level	Frequency	Percentage (%)
SPM	0	0
STPM	2	10
Bachelor Degree	13	65
Master	0	0
PHD	0	0
Others	5	25
	20	100

4.2.6 Statistical Analysis of Demographic Data

Table 4.6 shows the statistical analysis of demographic data. It shows the mean, median and mode of the respondent's age are 36.44, 36.5 and 33 respectively. The mean, median and mode of working experience is 10.5, 9 and 6 respectively. The mean of respondent's working department in company is 2.8572 while median is 3 and mode is 3. The highest level education achieves mean 3.3333, median 1 and mode is 0.

Table 4.6: Statistical analysis of demographic data

Items	Mean	Median	Mode	Standard Deviation
Age	36.55	36.5	33	6.3534
Working Experience	10.5	9	6	7.1562
Department	2.8572	3	3	1.3452
Highest Level Education	3.3333	1	0	5.1251

The summary of respondents' background is show in Table 4.7 as below.

Table 4.7: Summary of respondents' background

Respondent	Gender	Age	Department	Working Experience (years)	Highest Level of Education
1	Male	28	IT	6	Degree
2	Male	29	IT	10	Degree
3	Female	33	Warehouse	5	Degree
4	Female	31	Warehouse	9	Degree
5	Female	41	Marketing	20	Degree
6	Male	32	IT	9	Others
7	Female	27	R&D	2	Degree
8	Female	41	R&D	23	Degree
9	Male	48	IT	25	Degree
10	Female	45	IT	24	Degree
11	Male	33	Warehouse	5	Degree
12	Female	36	R&D	7	Others
13	Male	38	Marketing	8	Others
14	Female	37	Human Resource	6	Degree
15	Female	29	Human Resource	2	Degree
16	Male	40	R&D	10	Degree
17	Female	42	Human Resource	11	Others
18	Female	45	Supply Chain	13	Others
19	Male	43	Operation	12	STPM
20	Female	33	Supply Chain	3	STPM

4.3 TYPES OF RISKS IN IT SYSTEM

4.3.1 Natural Threats

Table 4.8: Natural threats in IT system

Natural Threat	Never	Rarely	Every once in a while	Sometimes	Almost Always	Total
Natural Disaster	6	8	5	1	0	20
Secondary Disaster	6	7	7	0	0	20

Form the table 4.8, most of the respondents thought that natural disaster is rarely occurred in IT system, which contributed 40% (8 people). Some of the respondents thought that natural disaster will never become a threat in IT system, which is 30% (6 people). Based on their opinions, Malaysia is a country that free of the natural disaster like earthquake and hurricanes. They believed that the company will have a proper preparation to overcome the natural disaster like fire. So, natural disasters will not be the main threat in IT system. However, there was 5 respondents (25%) thought the natural disaster will occur every once in a while. They considered the companies in Kelantan and Terengganu will face the flooding problem in the end of the year. The flooding problem may destroy the hardware and software system which probably could lead to partial or total outage. There were only 1 respondent (5%) felt that it will occur sometimes and nobody felt the natural disaster will always occur.

Table 4.8 shows that most of the respondents thought that secondary disaster is rarely occurred or occurred every once in a while. Both are 35% (7 people). The second disasters are successive disaster which result from the environment condition or natural disaster. In their opinions, broken water pipe is rarely occurred or occur every once in a while which may cause the internal flooding. Some of them felt that the water may split over accidentally when the cleaner was cleaning the office. That may cause the destruction of the hardware of the computer. The rest of the respondents which is 30% (6 people) felt that the second disaster would never occur in their office. Most of them considered the company has perfect equipment and preparation to overcome those situations.

4.3.2 Human Threats

Table 4.9: Human threats in IT system

Human Threat	Never	Rarely	Every once in a while	Sometimes	Almost Always	Total
Data entry errors or omissions	0	5	6	7	2	20
Espionage	9	3	6	2	0	20
Inadvertent acts or carelessness	2	4	8	4	2	20
Terrorism	9	6	4	1	0	20
Theft, sabotage, vandalism or physical intrusions	4	6	7	3	0	20

Table 4.9 shows that most of the respondents which contributed 35% (7 people) agreed that data entry errors or omissions will occur sometime. This is because they felt that people will do mistakes sometime especially during the peak period. However, the respondents said that this mistake will become a serious threat in IT system as the error of data entry will cause the data inconsistency. There are 6 people (30%) thought that data entry errors will occur every once in a while and 5 people (25%) thought that this threat is rarely occur. This is because they felt that people will make mistake easily but this mistake can be prevent from happen. There are only 2 people (10%) felt that this threat will occur almost always.

In table 4.9, there are 9 people (45%) thought that espionage will never happen in their company. This is because they believed that all the employees have the awareness about espionage is illegal. Besides, the respondents felt that the company will have preparation for this threat to prevent the information disclosure. There are 6 people (30%) thought that this threat will occur every once in a while as they considered that the competitors will try to get the useful information from the company to get the competitive advantage in the market. There are a few respondents considered this threat will rarely occur or happen in sometime which are 3 people (15%) and 2 people (10%) respectively.

Table 4.9 shows that there are 8 people (40%) thought that inadvertent acts or carelessness will occur every once in a while. Based on their opinions, they felt that many things happened accidentally and out of the control sometime. The people may not have the intention to create the problems. However, they believed that the employees recruited by company are professional enough on doing their work and handle the problems. There are 4 people (20%) felt that this threat will rarely happen or occur sometimes. There are only 2 people (10%) thought that this threat will occur almost always.

In table 4.9, most of the respondent (9 people, 45%) thought that terrorism will never occur in the company. This is because the political situation in Malaysia is quite stable and the possibility of terrorism occurs is quite low. There are 6 people (30%) thought that this threat will rarely occur and 4 people (20%) thought it will occur once a while. Based on their opinion, the terrorists nowadays are professional in IT and they may hack into company webpage or system to get the information they want or spread any news. There is only 1 person (5%) thought that it will occur sometime. However, most of the respondents considered that terrorism threat is rarely occur in normal business company.

There are 7 people (35%) thought that theft, sabotage, vandalism or physical intrusions will occur every once in a while in table 4.9. Based on their opinions, some of the disgruntled employees could create both mischief and sabotage of system data. They can destroy the computer system by installing software that could damage system or the data. There are 3 people (15%) felt that this threat will occur sometimes. However, there are 4 people (20%) thought that it will never occur in the company. Some of the respondents (6 people, 30%) felt that it will rarely occur. This is because they believed that the employees will not do the thing that does not bring any benefit for them. Based on their opinions, those disgruntled employees are formed by the employees that being lay off. However, they believed that the company will give the reasonable compensation to those employees. So, the probability of this threat to occur is very low.

4.3.3 Environmental Threats

Table 4.10: Environmental threats in IT system

Environmental Threat	Never	Rarely	Every once in a while	Sometimes	Almost Always	Total
EMI	2	9	7	2	0	20
Environmental conditions	4	6	7	3	0	20
Hazardous material accident	4	8	7	1	0	20
Physical cable cuts	7	7	5	1	0	20
Power Fluctuation	4	5	4	4	3	20

Table 4.10 shows that there are 7 people (35%) felt the Electromagnetic Interference (EMI) will occur every once in a while. There are 2 people (10%) felt that it occur in sometimes. Based on their opinions, they said EMI will normally cause the line noise which corrupted data transfer from CPU to disk, printing errors or affect the computer monitor screen. However, there are 9 people (45%) considered this threat is rarely happen in their company. There are 2 people (10%) thought that is never occur. They said their company is rarely affected by EMI problem.

In table 4.10, there are 7 people (35%) thought environmental threat will occur once in a while and 3 people (15%) felt it will occur in sometimes. They agreed that overheating in a computer rooms could cause the computer failure and downtime. There are 6 people (30%) felt that this threat is rarely occur in their company and 4 people (20%) considered that it will never happen. Based on their opinions, the office has air-conditioner and the overheating problem will rarely or never occur in the office. However, some of the respondents felt that the leakage of water from the air-conditioner will damage the computer equipment.

The hazardous material accident is rarely occurring for 8 respondents (40%). In table 4.10, there are 4 people (20%) felt that it will never occur in the company. They considered that most of the employees will not put the hazardous material especially the flammable things in the office. However, there are 7 people (35%) considered it will occur every once in a while and only 1 people thought it will occur in sometimes. Their opinions are the office cleaning materials may content flammable materials which can cause explosion if do not keep it at a specific temperature. Some of the respondents felt that the office cleaners may spill the cleaning materials when they are cleaning the office. So, the computer system may break down and unable to be functioned if computer hardware contacts with those chemical.

There are 7 people (35%) felt that physical cable cuts is rarely or never occur in the company which show in table 4.10. This is because most of the employees will back-up all their works. So, they have no worry about the electricity shut off suddenly. However, there are 5 people (25%) considered the physical cable cuts will occur once in a while and only 1 person (5%) felt that it will occur in sometimes. Based on their opinions, the physical cable cut is always caused by lightning strikes which could cause the circuits burn out. This would result in power failure and cause the computer system break down.

In table 4.10, there are 4 people (20%) considered power fluctuation will never occur in the company and 5 people (25%) felt that is rarely occur. This is because most of the respondents believed that employees will back up all their works. The sudden black out will not have much impact for them. However, there are 4 people (20%) considered this threat will occur every once in a while and sometime respectively. There are 3 people (15%) felt that it occurs almost always. Based on their opinions, a power outage could affect the malfunction of CPU and system which will bring a large impact on timeliness and quality of the delivered service.

4.3.4 Technical Threats

Table 4.11: Technical threats in IT system

Technical Threat	Never	Rarely	Every once in a while	Sometimes	Almost Always	Total
Corruption by system, system errors and failure	3	2	6	5	4	20
Data or system contamination	2	5	6	4	3	20
Eavesdropping	2	4	10	3	1	20

Table 4.11 shows that there are 6 people (30%) felt that corruption by system, system errors and failure will occur every once in a while in their company. Based on their opinions, system failure is caused by the pure automation approach. The system may upgraded automatically and cause a temporary system break down. There are 5 people (25%) felt that this threat will occur in sometimes and 4 people (20%) considered it will occur almost always. Since not all the employees are expertise in IT field, so, when system failure, the employees only can wait for the IT technician to repair it. However, some of the respondents felt that this threat will never occur which is 3 people (15%). There are 2 people (10%) agreed that the threat is rarely occur. This is because their tasks can be conducted manually. So, system failure can consider not the main threat for them.

In table 4.11, there are 6 people (30%) felt that data or system contamination is occurred every once in a while. Some of the respondents (4 people, 20%) felt that it is occurred in sometimes and 2 people (10%) said it will occur almost always. Based on their opinions, computer virus can cause the system contaminated. The computer virus attaches itself to targeted computer’s system and replicated itself automatically and spread to other computers. So, the system contamination can occur easily. However, there are 3 people (15%) felt that this threat will never occur in the company and 5 people (25%) felt that it is rarely occur. This is because most of the company’s computer had installed anti-virus software. It can prevent the computer from attack by the virus which can cause the system contamination.

The table 4.11 shows that there are 5 people (25%) felt that eavesdropping can occur every once in a while. 3 respondents (15%) felt that it may occur in sometimes and only 1 person (5%) felt that it will occur almost always. In their opinions, eavesdropping devices such as Electronic Bugs can be used to intercept sensitive and unencrypted data. However, there are 8 people (40%) felt that it will never occur in the company and 3 people (15%) felt that it is rarely occur. This is because they believed that the IT technicians in the company can detect if there are any eavesdropping devices and do some preparation to prevent the protected data being disclosure.

4.3.5 Other Risks

Based on the respondents' opinions, lack of computer skills and knowledge is another threat in IT system. Some of the employees may not expertise in using computer and they may make some mistakes when they are using the computer. It is importance that the employees have to familiar with the hardware, operating system, databases and application software to prevent a huge mistake is occurred.

Besides, the respondents considered that the system is not user friendly is another threat in IT system. In their opinions, company will use the new system after the old system had been use for several years. Therefore, the new system should be user friendly as the employees can learn to use it easily.

The other threat is poor website or network design. The respondents said that the poor network design can allow the hackers to hack into the webpage easily and get the data from the system. This will cause the data and important information being disclosed.

Summary of the type of risks in IT system is showed in Table 4.12 as below.

Table 4.12: Summary of the types of risks in IT system

Type of Risks in IT System	Scale Range									
	Never	%	Rarely	%	Every once in a while	%	Sometimes	%	Almost Always	%
Natural disaster	6	30.00	8	40.00	5	25.00	1	5.00	0	-
Secondary disaster	6	30.00	7	35.00	7	35.00	0	-	0	-
Data entry errors or omissions	0	-	5	25.00	6	30.00	7	35.00	2	10.00
Espionage	9	45.00	3	15.00	6	30.00	2	10.00	0	-
Inadvertent acts or carelessness	2	10.00	4	20.00	8	40.00	4	20.00	2	10.00
Terrorism	9	45.00	6	30.00	4	20.00	1	5.00	0	-
Theft, sabotage, vandalism or physical intrusions	4	20.00	6	30.00	7	35.00	3	15.00	0	-
EMI	2	10.00	9	45.00	7	35.00	2	10.00	0	-
Environmental conditions	4	20.00	6	30.00	7	35.00	3	15.00	0	-
Hazardous material accident	4	20.00	8	40.00	7	35.00	1	5.00	0	-
Physical cable cuts	7	35.00	7	35.00	5	25.00	1	5.00	0	-
Power Fluctuation	4	20.00	5	25.00	4	20.00	4	20.00	3	15.00
Corruption by system, system errors and failure	3	15.00	2	10.00	6	30.00	5	25.00	4	20.00
Data or system contamination	2	10.00	5	25.00	6	30.00	4	20.00	3	15.00
Eavesdropping	2	10.00	4	20.00	10	50.00	3	15.00	1	5.00

4.4 IMPACT OF RISK MANAGEMENT IN IT SYSTEM

Table 4.13: Impact of risk management in IT system

Impact	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
Data integrity	0	4	2	5	9
Confidentiality of data	0	1	6	3	10
Availability of data	0	1	5	9	5
Simplified report building and analytics	0	2	3	11	4
Better operational efficiency	1	2	1	12	4

Table 4.13 shows that there are 9 people (45%) strongly agree and 5 people (25%) somewhat agree with the data integrity is one of the impact of risk management in IT system. Based on their opinions, risk management in IT system can ensure that the data in the system to maintain in the correct signs and symbols. This can prevent the inaccuracy of data in the system in order to ensure the system can be used smoothly. There are 2 people (10%) felt neutral on this impact. However, there are 4 people (20%) felt somewhat disagree with it. In their opinions, most of the integrity lost is caused by the human errors. Although there is a regular risk management in IT system, but the data integrity is not corrected within that period and the problem of the system is still appeared.

In the table 4.13, most of the respondents (10 people, 50%) are strongly agree with the confidentiality of data as an impact of risk management in IT system. There are 3 people (15%) who somewhat agree with this impact. The respondents felt that risk management can prevent the data from unauthorised disclosure. The IT technicians can detect if there is any hacker hacking into the system and prevent the data being disclosed. There are 6 people (30%) felt neutral on this and only 1 person (5%) felt somewhat disagree with this. Based on the respondent’s opinion, everyone has their own account to log into the company system. However, some of them may forget to log out when they left and this will give the chance for others to get the information without permissions.

Table 4.13 shows that there are 9 people (45%) somewhat agree and 5 people (25%) strongly agree with the availability of data as the impact of risk management in IT system. Most of the respondents felt that risk management in IT system can ensure that the systems remain available when they are needed. They felt that availability of data is quite important in the company as they need to use the system for their daily work tasks. So, the risk management in IT system can prevent the system failure. There are 5 people (25%) felt neutral on this and only 1 person (5%) somewhat disagree with this. The respondent felt that the system break down still occurred during work time although the risk management in IT system is applied.

There are 11 people (55%) somewhat agree and 4 people (20%) strongly agree with the simplified report building and analytics as the impact of risk management in IT system which showed in table 4.13. Most of the respondents agreed that the system standardised all the data into common format make their work become easier. Risk management can ensure that the data can be filtered and it is in the same format when the report is needed. There are 3 people (15%) felt neutral on this and 2 people (10%) felt somewhat disagree with this. This is because the system may goes wrong sometime.

In table 4.13, there are 12 people (60%) somewhat agree and 4 people (20%) strongly agree with risk management in IT system brings a better operational efficiency to the company. The respondents agreed that risk management ensure the employees can enter into the same online system simultaneously to get the data they want. This can improve the performance of work. There are 1 person (5%) felt neutral in this. However, there are 2 people (10%) felt somewhat disagree and 1 person (5%) felt strongly disagree with this. The respondents felt that everyone can enter the system at the same time which will cause the system become slower and it will delay their work.

4.4.1 Other Impact of Risk Management in IT System

The other impact of risk management in IT system from respondents' view is faster decision making. The company usually will use "one system" approach which means all the departments are using the same system. This can ensure that the employees enter to the data which is continually and instantly updated. The advantage of this is it enables quicker identification of patterns in data, therefore the actions and controls can be taken immediately.

Another impact of risk management in IT system which given by the respondents is traceability of data. Based on the respondents' opinions, the data entered in one section will always be from the original source and can be traced back to who entered it and when the data is entered. By implement the risk management in IT system, the employees can check the values entered whether there is any error and then alert the necessary employees.

4.4.2 Method to Increase Impact of Risk Management in IT System

Based on the opinion of respondents, they suggested that regular evaluation of IT system can increase the impact of risk management in IT system. Regular evaluation can ensure the system is up to date with the latest technology to deal with all kinds of threats. Regular evaluation can find out the weakness of the system and take the immediate action to improve that particular area.

Another method is using anti-malware and spyware program. By using this program, it can help the computer to identify the virus and other problematic files which will infect the computer system. Therefore, it can ensure the computer system is secure.

Summary of the result of impact of risk management in IT system is showed in table 4.14 as below.

Table 4.14: Summary of the result of impact of risk management in IT system

Impact of Risk Management in IT system	Scale Range										(1-2) %	3%	(4-5) %	Classification
	1	%	2	%	3	%	4	%	5	%				
Data integrity	-	0.00	4	20.00	2	10.00	5	25.00	9	45.00	20.00	10.00	70.00	Agree
Confidentiality of data	-	0.00	1	5.00	6	30.00	3	15.00	10	50.00	5.00	30.00	65.00	Agree
Availability of data	-	0.00	1	5.00	5	25.00	9	45.00	5	25.00	5.00	25.00	70.00	Agree
Simplified report building and analytics	-	0.00	2	10.00	3	15.00	11	55.00	4	20.00	10.00	15.00	75.00	Agree
Better operational efficiency	1	5.00	2	10.00	1	5.00	12	60.00	4	20.00	15.00	5.00	80.00	Agree

4.5 CONCLUSION

The data analysed in this chapter is collected by sending email to the company and interview section is conducted. The chapter started with the respondents' information which is included the age, gender, working experience, department and the highest level of education. There are totally 20 respondents selected in the company. After that, the types of risks in IT system were analysed. Besides, the impact of the risk management in IT system was analysed too. Lastly, the method to increase the impact of risk management in IT system which was suggested by the respondents was analysed.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

In this chapter, discussions of result, limitation and recommendation for future research and the conclusion had been carried out. The discussion of result is concluding the two research questions. The limitation is covering the limitation from research and researchers. The recommendations are for managerial practice and future research based on the conclusion. This research mainly is to study types of risk in IT system and the impact of risk management in IT system.

5.2 DISCUSSION

There are two objectives in this research. Firstly is to identify the risks in IT system that influence the performance of organization. The second objective is to determine the impacts of risk management in IT system to the organization. All the two research objectives (RO) are achieved successfully.

RO1: Identify the risks in IT system that influence the performance of organization

Firstly, this research discusses the result obtained by analysing the risks in IT system. In this research, there are 15 risks in IT system and had been classify into 4 groups which included natural threat, human threat, environmental threat and technical threat.

From previous chapter, based on 20 respondents, the five risks which most frequently occurred in IT system that will influence the performance of organization were data entry errors or omissions, corruption by system, system errors and failure, inadvertent acts or carelessness, data or system contamination and lastly power fluctuation.

Most of the respondents agreed that data entry errors or omission is one of the risks that most frequently occurred in IT system. People will make mistake especially during the peak working period. There are few reasons of data entry errors or omission. Due to sit in front of the computer to key in all the data can cause the tiredness of the eyes which easily lead to data entry errors or omission. However, this mistake will affect the performance of organization as the data inconsistency. Besides, respondents also agreed that corruption by system, system errors and failure is another significant risk in IT system. The system may upgraded automatically and cause a temporary system break down. This threat will delay the progress of work and influence the performance of organization.

Apart from that, respondents also agreed that inadvertent acts or carelessness in IT system will influence the performance of organization. This unintentional act will cause the system performance degradation or system loss. For example, incorrect operations of database synchronization process may cause in data errors which are including entry, deletion and corruption errors. In addition, data or system contamination is another risk in IT system which will affect the performance of organization. The viruses in the computer will intermixing the data of different sensitivity levels which could affect the progress of work and data integrity problem. Respondents agreed that power fluctuation will influence the performance of organization. A power outage could affect the timeliness and quality of the delivered service which definitely will affect the performance of the organization.

There are some risks in IT system had mentioned by the respondents which including lack of computer skills and knowledge, new system is not user friendly and poor website or network design. Most of the respondents agreed that not all the employees are expertise in using computer system. Lacking of computer skills and knowledge could make them did some mistakes when they are using the operation system. This could delay the progress of work and influence the performance of organization. Besides, new system which is not user friendly is another risk in IT system. This is because employees have to use more time to learn how to use the new system for their daily work. This will affect the progress of work. Last but not least, respondents considered the poor website or network design is the risk in IT system. The hackers can hack into the network of the company easily if the design was poor. This will lead to the important information disclosure and affect the company's performance.

RO2: Determine the impacts of risk management in IT system to the organization

In this section, the researcher discusses about the impacts of risk management in IT system to the organization. There are 5 impacts of risk management in IT system which are data integrity, confidentiality of data, availability of data, simplified report building and analytics and better operational efficiency. From 20 respondents, 3 most significant impacts of risk management in IT system are better operational efficiency, simplified report building and analytics, and availability of data.

Majority of the respondents agreed that better operational efficiency is one of the significant impacts of risk management in IT system. Employees can enter into the same online system simultaneously for their daily work. By using multiple systems and databases, employees can perform the manual quality checks and maintenance for their data. Besides, the other significant impact of risk management in IT system is simplified report building and analytics. By implement risk management in IT system, the data can be standardised into common format especially when the data is in multiple currencies and different languages. The other important impact of risk management in IT system is availability of data. By implement the risk management in IT system, the data in the system can be available to its end user and it will increase the performance of employees in supporting the organization's mission.

The other impacts of risk management in IT system that mentioned by respondents are faster decision making and traceability of data. Respondents agreed that risk management in IT system can help the employees enter to system continually and the data is instantly updated. Risk management in IT system help the company in tracing the data. The data entered can be traced back to who entered it and when the data is entered. Therefore, the management can check whether there is any error.

Respondents mentioned that regular evaluation of IT system is very important. Regular evaluation can determine the weakness of the system and the system can be upgraded to overcome all the threats. Some of the respondents suggested that using anti-malware and spyware program in the computer system. It can help to identify the virus in the computer and secure the computer system.

5.3 LIMITATION AND RECOMMENDATION

There are various limitations in this research. One of the limitations is time. Researcher is given a limited time to complete the research. However, a research is complicated and need a long time to complete it. The time available for doing this research is limited. As a university student who needs to fulfil their responsibility to complete the other subjects, researcher cannot put fully commitment to this research. Therefore, in the future research, researcher should be given sufficient time in order to complete the research.

Furthermore, the respondents of this research are targeted on one company in Johor Bahru only. All the data is collected more from the interview. Thus, the data just collected from one company may affect the result from this research may not very accurate and significant due to limited respondents. The respondents may give their opinions based on their memory, self-favourable and personal judgement. Therefore, in the future research, researcher can expand their population to other companies in order to increase respondent rates and get more data from respondents.

Other than that, difficulties in collect back data also one of the limitations of this research. In this research, 20 respondents had been selected randomly. The questionnaires had been sent out before an interview is conducted. However, the respondents were busy working with their tasks and the interview section was distracted. It consumed a lot of time to collect all the data as the researcher had to assort the time with the respondents. In the future research, researcher can make appointment with the respondents rather than walk-in interview. So, the respondents can focus during the interview session.

In addition, the knowledge is another limitation of this research. This research is about the risk in IT system. However, everyone has different levels of knowledge in IT system. Everyone’s knowledge is limited and different people are expert in different fields. The insufficient study of the researcher may cause the data analysis inaccurate since the research is based on the knowledge of researcher. In the future research, researcher should read a lot journal or articles which related to the topic and select the respondents who have the knowledge on that particular area rather than random selected.

Apart from that, this research only used questionnaire, interview and documentation to collect data. In the future research, more methods can be used to increase the accuracy and reliability of the data. For example, future researcher can use both qualitative and quantitative research. Similarity, this research only studies a company in Johor Bahru. Further study can be covered more areas in Malaysia in order to get the more accurate results.

Lastly, the research showed that risk management in IT system can help the company to improve the performance. Risk management can be concluded as one of the key determinants of better performance of organization. However, this research only studies on risk management in IT system due to limitation of time and cost. Therefore, the future research can do at more areas in order to study the relationship of risk management and better performance of organization.

5.4 CONCLUSION

As conclusion, this research is to investigate the type of risk in IT system and the impacts of risk management in IT system to the organization. Through the questionnaire survey and interview session, the risk that most frequently occurred in IT system and the significant impacts of risk management in IT system were identified. There are four groups of types of risk in IT system which are natural threat, human threat, environmental threat and technical threat. Overall, respondents agreed that human threat is the risk the most frequently occurred in IT system. In addition, there are five impacts of risk management in IT system which are data integrity, confidentiality of data, availability of data, simplified report building and analytics and better operational efficiency. In overall, respondents agreed that better operational efficiency is the most significant impact of risk management in IT system. Based on this research, the researcher can identify which risks are always occurred and find out the solution to reduce these threats. Besides, risk management in IT system brings a lot of benefit to organization. Therefore, risk management in IT system has to be conducted continually to ensure a better performance of organization.

REFERENCES

Adeleye, B. C., Annansingh, F., & Nunes, M. B. (2004). Risk management practices in IS outsourcing: an investigation into commercial banks in Nigeria. **International Journal of Information Management** 24(2), 167-180.

Adnan, H. (2009). An assessment of risk management in joint venture projects (JV) in Malaysia. **Asian Social Science** 4(6), p99.

Akintoye, A. S., & MacLeod, M. J. (1997). Risk analysis and management in construction. **International Journal of Project Management** 15(1), 31-38.

Azizan, M. A., & Ibrahim, F. A. (2015). Implementation of Risk Management in Malaysia Design and Build Projects. **Advances in Environmental Biology** 9(3), 108-111.

Baccarini, D., & Archer, R. (2001). The risk ranking of projects: a methodology. **International Journal of Project Management** 19(3), 139-145.

Bahli, B., & Rivard, S. (2001). An assessment of information technology outsourcing risk. **ICIS 2001 Proceedings** 74.

Boiney, G. L. (1999). Knowledge is Power: but knowledge management requires organizational change. **Journal of Contemporary Business Practice, Spring 1999** [Online] Available at: http://gbr.pepperdine.edu/992/infotech.html [Accessed 10 April 2015]

Broady-Preston, J. & Hayward, T. (2001). Strategy, information processing and scorecard models in the UK financial services sector. **Information Research** [Online] **7**(1) Available at: http://InformationR.net/ir/7-1/paper122.html [Accessed 11 April 2015]

Buc, D., Corbier, J., Eric, D., Jean-Philippe, J., & Gerard, M. (2009). **Risk Management – Concepts and Methods** 1-40

Cervone, H. F. (2006). Project risk management. **OCLC Systems & Services: International digital library perspectives** 22(4), 256-262.

Close, D. B. (1974). An organization behavior approach to risk management. **Journal of Risk and Insurance** 435-450.

Cloutman, S. (2015). **6 advantages of unifying data into a risk management information system** [Blog.ventivtech.com]. Available at: http://blog.ventivtech.com/blog/6-advantages-of-unifying-data-into-a-risk management-information-system [Accessed 6 April 2015]

De Vaus, D. A., & de Vaus, D. (2001). **Research design in social research**: Sage.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. **Communications of the ACM** 43(7), 125-128.

Dictionaries, (n.d.). O. **"$pageTitle". Oxford Dictionaries**: Oxford University Press.

Dowie, J. (1999). Against risk. **Risk Decision and Policy** 4(1), 57-73.

Đurković, O., & Raković, L. (2009). Risks in Information Systems Development Projects. **Management** 4(1), 013-019.

Elky, S. (2006). An Introduction to Information System Risk Management. **SANS Institute InfoSec Reading Room.**

Gray C.F & Larson E.W. (2008). Managing Risk. **Project management the managerial process** 4th edn, McGraw-Hill/Irwin, New York, pp. 197-215

Hillson, D. (2003). **Effective opportunity management for projects: Exploiting positive risk**: CRC Press.

Information technology systems. (n.d.). **McGraw-Hill Dictionary of Scientific & Technical Terms, 6E** (2003) [Online]. Available at: http://encyclopedia2.thefreedictionary.com/Information+technology+sysems [Accessed 30 March 2015]

Islam, M. A., & Tedford, D. (2012). Implementation of risk management in manufacturing industry-An empirical investigation. **People** 2(3).

Kwak, Y. H., & Stoddard, J. (2004). Project risk management: lessons learned from software development environment. **Technovation** 24(11), 915-920.

Larman, C. (2004). **Agile and iterative development: a manager's guide**: Addison-Wesley Professional.

Markgraf, B. (2015). Importance of Information Systems in an Organization**. Small Business - Chron.com** [Online]. Available at: http://smallbusiness.chron.com/importance-information-systems-organization-69529.html [Accessed 16 March 2015]

Nikolić, B., & Ružić-Dimitrijević, L. (2009). Risk assessment of information technology Systems. **Issues in Informing Science and Information Technology** 6, 595-615.

Organizational Performance. (n.d.). **BusinessDictionary.com** [Online]. Available at: http://www.businessdictionary.com/definition/organizational-performance.html [Accessed 30 March 2015]

Patterson, F. D., Neailey, K., & Kewley, D. (1999). Managing the risks within automotive manufacturing. **Risk Management** 7-23.

PMI . (2013). **A Guide to the Project Management Body of Knowledge: PMBOK(R) Guide** 5th ed.Project Management Institute

Pons, D.J. (2010). Strategic Risk Management: Application to Manufacturing. **The Open Industrial & Manufacturing Engineering Journal** 3, 13-29.

Project Management Institute (2008) **A Guide to the Project Management Body of Knowledge (PMBOK)** 4th ed., Project Management Institute, Newtown Square (PA).

Raz, T., Shenhar, A. J., & Dvir, D. (2002). Risk management, project success, and technological uncertainty. **R&D Management** 32(2), 101-109.

Research-methodology.net,. (2015). **Exploratory Research - Research Methodology** [Online]. Available at: http://research-methodology.net/research methodology/research-design/exploratory-research/ [Accessed 10 April 2015]

Ronald, E.S.K. (2004). Project Risk Management. **Atlanta International University, Project Risk Management.**

Seifert, L. (2014). Project Risk Management For Design-And-Build Construction Projects.

Sekaran, U., & Bougie, R. (2010). Research methods for business: A skill building. **Chichester, West Sussex: John Wiley & Sons, Inc.**

Sicotte, C., Paré, G., Moreault, M.-P., & Paccioni, A. (2006). A risk assessment of two interorganizational clinical information systems. **Journal of the American Medical Informatics Association** 13(5), 557-566.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. **Nist special publication** 800(30), 800-830.

The MITRE Corporation, (2015). ***Risk Management Approach and Plan*** [Online]. Available at: http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-approach-and-plan [Accessed 9 April 2015]

Vancouver Island University, (2015). **5 Steps of Enterprise Risk Management – Risk Management | Vancouver Island University (VIU)** [Online]. Available at: https://www2.viu.ca/riskmanagement/identification.asp [Accessed 9 April 2015]

Ward, S., & Chapman, C. (2003). Transforming project risk management into project uncertainty management. **International Journal of Project Management** 21(2), 97-105.

Williams, L. (2004). Risk Management. **Project Risks Product-Specific Risks** 1-22.

APPENDIX A

COVER LETTER FOR QUESTIONNAIRE

UMP
Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

Dear Sir/Madam,

This is an academic study to fulfil one of the requirements of Final Year Project under Bachelor Degree of Project Management course in University Malaysia Pahang. The study is to identify the type of risks in IT system and the impact of the risk management in IT system to the organizations.

2. Enclosed with this letter is a questionnaire that consists of 3 sections. Section A is respondent profile, Section B is type of risk in IT system and Section C is the impact of risk management in IT system to organizations. Your response to the survey is important to succeed the research. Your answer and identity will be confidential and will be used only for the academic research purpose. Your cooperation in answering this questionnaire will be much appreciated.

3. If you have any queries or concerns about completing the questionnaire, you may contact me at 010-8017708 or janetsu1007@gmail.com.

Yours truly,

SU HUI MIN
Std. ID: PB12038
Faculty of Industrial Management
University Malaysia Pahang

APPENDIX B

QUESTIONNAIRE

SECTION A: PERSONAL INFORMATION

1. Name: ____________________________
2. Age: ___________________
3. Gender: Female / Male
4. Working Experience in IT: ____________________ year(s)
5. Department in Company: ___________________________
6. Higher Level of Education: ☐ SPM

   ☐ STPM

   ☐ Bachelor Degree

   ☐ Master

   ☐ PHD

   ☐ Others, please state: _____________________

SECTION B: TYPES OF RISKS IN IT SYSTEM

Using the following scale, please answer each of the following questions by circle in the appropriate box. **What are the risks in IT system? How frequently they occurred in organization?**

1. Never	2. Rarely	3. Every once in a while	4. Sometimes	5. Almost always

A. Natural threats					
i. Natural disaster	1	2	3	4	5
ii. Secondary disaster Eg: Spilled chemicals can cause a fire.	1	2	3	4	5

B. Human threats						
iii.	Data entry errors or omissions	1	2	3	4	5
iv.	Espionage	1	2	3	4	5
v.	Inadvertent acts or carelessness	1	2	3	4	5
vi.	Terrorism	1	2	3	4	5
vii.	Theft, sabotage, vandalism or physical intrusions	1	2	3	4	5

C. Environmental threats						
viii.	Electromagnetic Interference (EMI)	1	2	3	4	5
ix.	Environmental conditions	1	2	3	4	5
x.	Hazardous material accident	1	2	3	4	5
xi.	Physical cable cuts	1	2	3	4	5
xii.	Power Fluctuation	1	2	3	4	5

D. Technical threats						
xiii.	Corruption by system, system errors and failure	1	2	3	4	5
xiv.	Data or system contamination	1	2	3	4	5
xv.	Eavesdropping	1	2	3	4	5

Other types of risks in IT system that often occurred (if have please state):

____

____

____

How frequent to implement risk management to IT system in your organization?

____

____

____

SECTION C: IMPACT OF RISK MANAGEMENT IN IT SYSTEM TO COMPANY

Using the following scale, please answer each of the following questions by circle in the appropriate box. **What are the impacts of risk management in IT system to organization?**

1. Strongly disagree	2. Somewhat disagree	3. Neutral	4. Somewhat agree	5. Strongly agree

i.	Data integrity	1	2	3	4	5
ii.	Confidentiality of data	1	2	3	4	5
iii.	Availability of data	1	2	3	4	5
iv.	Simplified report building and analytics	1	2	3	4	5
v.	Better operational efficiency	1	2	3	4	5

Other impact of risk management in IT system to company (if have please state):

____

____

____

How effective of the risk management in IT system?

____

____

____

Is it important to implement risk management in IT system in organization? If yes, please state the reason.

____

____

____

How to increase the impact of risk management in IT system?

____

____

____

Please attach your signature, name and phone number here to validate the participation in answering the questionnaire.

____

Name:

Phone Number:

Thank you very much for spending your time to complete this questionnaire. Your cooperation is much appreciated.

APPENDIX C

GANTT CHART FYP 1

NO	WEEK TASKS	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Meeting with SV to discuss the research title and objectives	■													
2	Find journal and information		■												
3	Preparing Chapter 1			■											
4	Preparing Chapter 2				■	■									
5	Preparing Chapter 3						■								
6	Adjustment and editing the draft							■							
7	Submit draft Chapter 1,2,3								■						
8	Preparing for presentation									■					
9	Presentation										■				
10	Correction											■	■	■	■

APPENDIX D

GANTT CHART FYP 1I

NO	Week Task	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Finalise questionnaire	■													
2	Distribute questionnaire		■												
3	Interview			■	■	■	■								
4	Analyse data							■	■						
5	Do the report								■	■	■				
6	Submission poster and finalise everything										■	■			
7	Submission FYP II and presentation												■	■	■