UNIVERSITAS INDONESIA

PROPOSE DISASTER RECOVERY PLAN FOR PT XYZ

THESIS

TJIO SIVA SHERWIN
0906586171

FACULTY OF ECONOMICS
MAGISTER OF MANAGEMENT PROGRAM
JAKARTA
JUNE 2011

UNIVERSITAS INDONESIA

PROPOSE DISASTER RECOVERY PLAN
FOR PT XYZ

THESIS

Submitted to fulfill one of the requirements to obtain degree of Master of Management

TJIO SIVA SHERWIN
0906586171

FACULTY OF ECONOMICS
MASTER OF MANAGEMENT PROGRAM
MM – MBA PROGRAM
JAKARTA
JUNE 2011

STATEMENT OF ORIGINALITY

This final paper represents my own effort, any idea or excerpt from other writers in this final paper, either in form of publication or in other form of publication, if any have been acknowledge in this paper in accordance to the academic standard or reference procedures

Name	: Tjio Siva Sherwin
Student Number	: 0906586171
Signature	:
Date	: 24 June 2011

LETTER OF APPROVAL

Proposed by
Name : Tjio Siva Sherwin
NPM : 0906586171
Study Program : MM – MBA
Title :

PROPOSE DISASTER RECOVERY PLAN FOR PT XYZ

Has successfully presented the thesis in front of Board of Examiner and is already approved as one of the requirements to achieve the title of Magister Management (MM) and Master of Business Administration (MBA) in Magister Management Study Program Faculty of Economy, Universitas Indonesia

BOARD OF EXAMINER

Counselor : Dr. Mohammad Hamsal (………………………)

Examiner : Dr. Tengku Ezni Balqiah (………………………)

Examiner : Dr. Rizal Edy Halim (………………………)

Place : Jakarta
Date : 19 July 2011

PREFACE

All praise and gratitude the writer turning to the presence of God Almighty for all the abundance of His blessing and grace so the writer can finish this thesis. The thesis is submitted to fulfill one of the requirements to obtain degree of Master of Management at Universitas Indonesia. The writer realizes that the results achieved so far cannot be separated from the help and support from various parties. Therefore, on this occasion the writer would like to express appreciation and gratitude as much as possible to:

1. Dr. Mohammad Hamsal, my thesis counselor who patiently guide me through this final phase of the program, with his support and suggestion;
2. Prof. Rhenald Kasali, PhD as Director of Magister Management Program of Faculty of Economics;
3. The Board of Examiners who have provided suggestions and constructive criticism for this thesis;
4. All lecturers and all staffs of MM-FEUI for their assistance and support during the period of my study in MM-MBA;
5. My family for all continuous support and encouragement especially my sister, Reva Sherwin whom contributes in completion of this thesis through her valuable feedback;
6. My fellow working colleagues (Meilani Setiawan, Agustina, Edo Sandy, and Icha for the support and patience);
7. Great class of MM-MBA 2009. Thank you for the great two years of knowledge sharing, discussion, and laughter.

The writer is fully aware that this thesis is far from perfect. Constructive critics, suggestions, and recommendations would cover the knowledge's constraint reflected in this thesis. Hopefully, this thesis provides benefits for the development of science.

Jakarta, 24 June 2011
Tjio Siva Sherwin

LETTER OF AGREEMENT TO PUBLISH THE THESIS FOR ACADEMIC PURPOSE ONLY

(Individual Assignment)

As a member of society of academicians of Universitas Indonesia, I have agreed as stated below:

Name	:	Tjio Siva Sherwin
NPM	:	0906586171
Study Program	:	MM-MBA
Faculty	:	Economy
Assignment type	:	Thesis

On behalf of science development, I have fully agreed to give the Non-exclusive Royalty Fee of the thesis to the Universitas Indonesia which titled:

PROPOSE DISASTER RECOVERY PLAN FOR PT XYZ

Along with any related materials if needed.

With this Non-exclusive Royalty Free Right, Universitas Indonesia has the right to keep, transform, and manage in form of database, distribute and publish it in the internet and other media as well for academic purpose only, even without permission as long as my name is mentioned and included as the sole writer/author and as the copyright holder.

Any form of lawsuit which possibly occur in the future event considered as copyright violation of this thesis will be my personal responsibility.

Sincerely I declare the statement above is true indeed.

Declared at Jakarta
On June, 24 2011

(Tjio Siva Sherwin)

ABSTRACT

Name : Tjio Siva Sherwin
Program Study : Master of Management – Master of Business Administration
Title : Propose Disaster Recovery Plan for PT XYZ

Surrounded with various endangering risks, businesses were forced to have a proper plan in place to ensure their businesses are well protected. Disaster recovery plan is one of the tools that can be utilized to protect businesses in particular IT function. The main purpose of this thesis is to identify PT XYZ's critical IT risks and propose recommendation from the existing disaster recovery. Recommendation is made based on theoretical framework based analysis obtained during study literature. This thesis is qualitative and descriptive research. The data was collected though observation and interview. This thesis suggests that there are several areas that need to be improved by PT XYZ such as regular updates on the plan whenever changes occured and expanding existing network bandwith capacity.

Key words:
Risk management, Business Continuity Management, Disaster Recovery Management, Information Technology

ABSTRAK

Nama : Tjio Siva Sherwin
Program Studi : Magister Manajemen – *Master of Business Administration*
Judul : *Propose Disaster Recovery Plan for PT XYZ*

Dikelilingi oleh berbagai resiko bisnis yang mengancam, perusahaan diperhadapkan pada suatu keharusan untuk memiliki suatu rencana agar bisnisnya tersebut tetap terlindungi. *Disaster recovery plan* merupakan salah satu alat yang dapat diutilisasi sebagai alat perlindungan khususnya untuk melindungi fungsi IT. Tujuan utama dari tesis ini adalah untuk mengidentifikasi risiko kritis IT PT XYZ dan mengajukan rekomendasi atas *disaster recovery plan* yang saat ini dimiliki PT XYZ. Rekomendasi dibuat berdasarkan analisa berbasis kerangka teori yang diperoleh saat studi literatur. Tesis in menggunakan metode penelitian bersifat kualitatif dan deskriptif. Data – data diperoleh lewat observasi dan wawancara. Tesis ini menghasilkan beberapa rekomendasi seperti *update* periodik atas *disaster recovery plan* ketika terjadi perubahan dan menambah kapasitas jaringan *network bandwith.*

Kata kunci:
Manajemen resiko, *Business Continuity Management, Disaster Recovery Management,* Teknologi Informasi

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

CHAPTER 1
INTRODUCTION

1.1 Background

It is now common to see that some firms had gone out from the business as their desired business goals are not achieved due to unforeseeable risks and stakeholders interests are not being properly accounted for.

Take the example of Arthur Andersen-Enron case whom both gone collapsed as they failed to manage their risks. Before its fall, Enron was lauded for its sophisticated financial risk management tools and was seen as a supply source for the best risk management experts and processes. In fact when revealed, Enron was found to do a high-risk accounting practices despite the fact that Enron's auditor, Arthur Andersen already regularly informed Enron their accounting practice invited scrutiny and presented a high degree of risk non-compliance with generally accepted accounting principles. The risk management established in place that is approval process for every projects were not fully followed in all cases and that the approval process was not well designed, including in the Special Purpose Entities transaction that triggering the off-balance-sheet event which then creates one of the big accounting scandal of all time (Rosen, 2003).

Also take the example of Japan as a country, as quoted from media, was known as the most earthquake-and tsunami-prepared country on the planet, now facing what the so called by media as the disaster trifecta – earthquake, tsunami and nuclear crisis (Begley & Murr, 2011). The impact of these catasthropes is worldwide and effected Japan's political, economic and psychological conditions (Bill, 2011).

These two examples set a good point that even those who prepared to deal with risks may falling apart. The question is what will happen if an organization is failing to prepare at all? These stories also highlight the importance for every organization to identify, understand and manage risks properly. Risks are not just a mere contextual jargon or discourse, but it must be a part of the organization, integrating and influencing throughout the organization.

Like it or not every business is exposed to various risks. The common company business risks could be categorized as strategic risks that is related to the way strategy is set and performance defined to implement this strategy; business or operational risks that is everything that happens in the core business units or services; compliance risks that is falling fouls of laws and regulations, or exposing the company to a legal claim of whatever nature; project risks that related to not delivering the project and as result not able to move forward (Pickett, 2006).

Many perceived risks as a form of uncertainty in business that both challenging and need to be conquered for the sake of business going concern. Some risks do can be mitigated but some are just unavoidable. In most cases, understanding threats and make preparation to deal with it, are proven contributory to lesser negative risk impact to a business.

The risks topic has increasingly gained his fame lately as disasters strike in many countries in the world and take up a lot of attention on how to prevent and mitigate this crisis in the future.

Risks has take its origin from uncertainty which affect one's objectives. In the past, Companies known this as threat. Recognising the needs to identify these risks/threats, Companies start to prepare their own risk assessment and learn ways to mitigate these risks. This is the beginning of risk management science where the risk assessments are now placed within a formal and standardized process. Enterprise Risk Management (ERM) comes next, where it tries to embed risk management throughout the organization (Pickett, 2006) and not a responsibility of risk department or risk officers only. The next derivative study is related to the Business Continuity Management (BCM). Initially, ERM is believed to be the umbrella process, whereas BCM provides the actual framework. But recently, this interconnectedness is being challenged. Power (2009: p 849) in his journal stated,

> "ERM has operated as a boundary preserving model of risk management subject to the 'logic of the audit trail', rather than a boundary challenging practice which confronts and addresses the complex realities of interconnectedness. The security provided by ERM is at best limited to certain states of the world and at worst it is illusory – the risk management of nothing. In contrast, Business Continuity Management (BCM) may provide clues about how risk management might be reconstructed."

The study of BCM are inarguably and explicitly help to overcome or mitigate risks in some of important business aspects as result of various disasters. One subcategory of BCM is Disaster Recovery Management (DRM). BCM aims to proactively manage all business processes, assets, facilities, supply chains, and human resources to ensure that the business will function at its highest capacity. This is distinct with DRM which concentrates on ensuring that IT contingency plans and procedures are in place to return to business as usual as soon as possible after a crisis (British Standard Institution, 2011).

Disaster Recovery Management became essential in our current world that is “dangerous” in the presence of disasters such as earthquakes, floods, tornadoes, pandemics, snow storms, fire and other natural disasters that can strike at any time and interrupt business important processes. Terrorism, riots, arson, sabotage, and other human created disasters can also damage the business. Accidents and equipment failures are also common to happen in daily lives (Wallace & Webber, 2011).

1.2 Statement of Problem

Surrounded with various endangering risks, businesses were forced to have a proper plan in place to ensure their businesses are well protected in the face of threats. Disaster Recovery Plan is one of the tools that an organization can utilized to better protect their assets and businesses.

There is a need to have a qualified disaster management within an organization. The symptoms are clear. As postulated by Elsner (2006) and Weart (2009), the world’s climate is changing at an alarmed rate (Thompson, 2010) In addition, terrorism, environmental pollution and the quest for energy have increased the potential for technological and natural hazards. Hazards, natural or man-made, can and often have catastrophic impacts on people’s lives and properties, physical infrastructures of societies, and the natural environment. According to the United Nations Environmental program (UNEP) there has been approximately 2,500 disasters in the world since the year 2000 that have resulted in millions of people losing their lives and cause millions of dollars in property damage on each impact. Disasters are not only unpredictable, but their impacts are also complex and difficult to understand and as a result difficult to manage. While it is very difficult to prepare for or mitigate disasters because of these complexities, it is still possible to manage their impact. Accordingly, disaster management organizations and systems must necessarily be complex to be effective. Understanding this, it is imperative that we try our best to improve organizations and systems to comprehensively manage hazards and the impacts (Thompson, 2010).

PT XYZ's parent group is one of the well-known brokering company in the world. As a servicing company, it provides consultancy services to its diverse clients. In doing business, PT XYZ realize in order be able to continue to function in the event of unforeseen interruption, the Company must have certain arrangements in place to meet their obligations as a business. It was believed that by implementing a Business Continuity Management (BCM), it will increase its recovery capabilities dramatically, can make the right decisions quickly, cut downtime and minimize financial losses. The whole idea of BCM is about preparedness. Having BCM in place demonstrates a duty of care to customers and suppliers, other stakeholders, safeguard reputation and at the same time will ensure the Company continue to operate and to meet legal, regulatory and contractual obligations.

PT. XYZ is a local subsidiary with ultimate parent company based in New York and listed in New York Stock Exchange. One of their line service is related to risk management consultancy in which they assist in for example adoption of ERM approach within client's organization and provide various BCM services such as review client's existing BCM program, Business Impact Analysis, Emergency Response Planning, Crisis Management Planning, and Business Recovery Planning. In light of the Company's expertise, it was then expected that the Company itself will, to certain extent, implement and maintain their minimum acceptable level of business continuity management as they suggested to their client. Failure in demonstrating and implementing effective business continuity management will have a tremendous impact over Company's reputation in the face of client and potential clients, especially for the line service Risk Consulting Group. This condition is potentially then be followed with lost sales, lost earnings, lost confidence/trust from related stakeholders and might impacted other line of services as well.

In consequence, PT. XYZ recognises risks as part of ongoing business and embrace it by having risk management policy and enforcing detailed plan to mitigate risks, as in the Company's disaster recovery plan (DRP) that is being part of Company's overall BCM. This thesis will further discuss the DRP as a plan, and areas of DRP that could be improved.

1.3 Purposes of the Study

1. To identify PT. XYZ's business risks especially IT risks.
2. To review current disaster recovery plan (DRP) and propose DRP for PT XYZ.
3. To provide suggestions on how to improve existing disaster recovery plan.

1.4 Benefits of the Study

The Company can be assured that the preventive measures taken through DRP are considered suffice to cope with disasters, based on studies taken in this thesis or the Company can enjoy improvement recommendation in their DRP, provided in last chapter of this thesis, which means better preparation in dealing with upcoming disasters that recently increased in terms of likelihood and severity. Due to it is complex nature, not all disasters can be fully contained but at least the Company through DRP will be able to reduce the impact to its ongoing business and minimize the financial loss. Specific benefits for the Company including:

- Stronger IT infrastructure. IT system can be recovered using specific best strategy available subject to Company's condition, needs and resources. This is important to protect the Company's data especially confidential ones.
- An increased protection to company's resources and minimize contractual obligations / financial losses.
- Business opportunities and raised reputation. For the Company is now perceived as being able to continue their business operations with

minimum disruption felt by stakeholders whilst competitors might not be able to do the same.

- Lower insurance premium as the risk now considered lower than before due to the existence of well-crafted DRP.

1.5 Method of Analysis

- Literature review, that is collecting relevant theories related to materials being discussed in this thesis to support the analysis.
- Observation, that is observing PT. XYZ and interviewing management to obtain the required data and information.

1.6 Study Limitation

It will focus mainly on IT risks and how the risks could be managed through a qualified disaster recovery plan. Beforehand there is no disaster occur in PT XYZ that requiring the Company to activate their DRP plan for IT Dept. Hence no benchmarking of the real capability or quality of its DRP in times of real disaster, is available. The scope analysis will mainly covered question of whether DRP implementation for IT Dept. is able to reduce risk of IT failure ?.

1.7 Framework Analysis

Chapter 1 Introduction

This chapter consists of background, problem formulation, purpose and benefits of the study, method of analysis and study limitation

Chapter 2 Literature Review

This chapter consists of supporting theories that provided framework as basis to do analysis. The theory used was mainly related to subjects of Risk Management, Enterprise Risk Management, Business Continuity Management and Disaster Recovery Management.

Chapter 3 Methodology

This chapter consists of methodology used to analyze PT XYZ's existing DRP. The author use the descriptive qualitative method as basis to elaborate the plan.

Chapter 4 Analysis

This chapter consists of general description of PT XYZ's establishment, business background and their risk management policy. The discussion followed with risk assessments including IT risks. Disaster recovery plan was then discussed as part of the overall business continuity management. Both are interrelated discussions. The final part of the chapter is discussing PT XYZ's disaster recovery plan based on data provided by management (including interview result) and the plan is analyzed using the theoretical framework provided in chapter 2.

Chapter 5 Conclusion and Recommendations

Based on facts and analysis found in Chapter 4, this chapter describes the Company's current practice or implementation of DRP, identify risks and provide recommendations to improve existing DRP.

CHAPTER 2
LITERATURE REVIEW

2.1 The Origin of Disaster Recovery Management

Disaster recovery management (DRM) was rooted from strategic management science. In the beginning, strategic management perspective is characterized as a long-term process for developing a continuing commitment to the mission and vision of an organization, nurturing a culture that identifies with and supports the mission and vision, and maintaining a clear focus on the organization's strategic agenda throughout all its decision processes and activities (Choi, 2009). Steiss (1985) views strategic management as the process whereby goals and objectives are identified, policies are formulated, and strategies are selected in order to achieve the overall purposes or mission of an organization. An important aspect of strategic management is its emphasis on organization adaptation to enviromental demands (Choi, 2009). This is relevant with DRM spirit which looks for ways to survive extreme business interruption, such as disaster. The ability to survive shows adaptability of the company to its environment in the face of threatening disasters.

How can we apply a strategic management perspective to emergency management ? Effective emergency management requires (Choi, 2009):

- Emergency management agencies and programs adapt and respond to enviromental uncertainties and demands on a continuous and ongoing basis
- Fundamental changes in organizational culture because emergency management practices involve profound changes in organizational values and ways of thinking.
- Time, resources, strong leadership commitment, and political support from inside and outside organizations
- Ongoing and active involvement of all participating organizations

An emergency management system can be strengthened by utilizing the strategic planning feature of strategic management. The challenge is how to apply underlying assumptions and elements of the strategic management approach to the current emergency management system in a manner that enhances organizational effectiveness and communities capacities in establishing an effective emergency management system. The most important thing is for us to understand strategic management features and to be more open and flexible to adopt new principles for present and future emergency management plans. By integrating strategic management to emergency management, the expected benefits are forward thinking, professionalization, capacity building through organizational learning and adaptation, goal identification and achievement through leadership and commitment, increased public support and accountability and more funding (Choi, 2009).

One of strategic management famous concept is SWOT analysis. This method of analysis can be used as a tool for organizations to assess their strategic position based on aspects such as strengths, weaknesses, opportunities and threats. Strengths and opportunities strategies are about using internal strengths to take advantage of external opportunities and contributes to value creation whilst weaknesses and threats strategies are defensive tactics directing at reducing internal weaknesses and avoiding enviromental threats (David, 2001). Weaknesses and threats creates risk for the company and hence there’s a need to analyze about its nature, likelihood and potential impact for the company to cope with it. Threat analysis is specifically discussed company’s weaknesses that out of the company’s control such as competitor. Threat analysis has a similar context with risk analysis in terms of both are discussing the obstacles inhibit the attainment of company’s goals. Pickett (2006) defined risk as any uncertainty about future events that impact an organization’s ability to achieve its objectives. Risk is usually measured in terms of its impact and the likelihood that it materializes. Wallace and Webber (2011) interprets risk analysis as a process that identifies the probable threats to the business. As time passes, it was started to realize that such risk analysis only as good as identifying risks on certain aspects that could affect the achievement of the desired objectives and no preventive measure yet in place. This concern which then evolves into risk management science whereas now there is a proactive mechanism in place throughout the organization that enables the Company to know new and changing risks that coming to our way and at the same time, enabling the Company to prepare themselves by having procedures or plan in place as a form of control to mitigate both existing and upcoming risks. Wallace and Webber (2011) interpret this process as risk assessment and define it as a process of comparing the risk analysis to the controls the Company have in place to identify areas of vulnerability.

Enterprise Risk Management (ERM) comes next where it tries to embed risk management throughout the organization. ERM as defined in www.coso.org, is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage the risks to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives. ERM definition as quoted from PT XYZ intranet is a structured and embedded approach that supports the allignment of strategy, processes, people, technology and knowledge with the purpose of evaluating and managing the uncertainties an organization faces as it creates value (Pickett, 2006).

Enterprise Resilience was the subsequent topic arise to overcome limitation of ERM. Conventional ERM help executives and directors focus on the nature of specific vulnerabilities and they can provide partial frameworks to help firms protect potentially weak links from low probability catastrophic risks. But they do not fully prepare companies for the discontinuities that can jeopardize earnings drivers. Conventional ERM fails to account for interdependencies accross vertical and horizontal corporate operations and thus tends to underestimate the range and severity of risks faced by the firm. In sharp contrast to traditional ERM, enterprise resilience planning advances a company's speed and flexibility by crafting an integrated first line of defense and offensive strategy to guard the entire extended enterprise against new, unavoidable risks that are the byproducts of interdependent operations. Resilient organizations are sensing, agile, networked and prepared. A resilient organization is able to (Starr, Newfrock and Delurey, n.d.):

- Effectively alligns its strategy, operations, management systems, governance structure and decision support capabilities so that it can uncover and adjust to continually changing risks.
- Endure disruptions to its primary changing earning drivers, and create advantages over less adaptive competitors.
- Establishes transparency and puts in place controls for CEOs and boards to address risks across the extended enterprise
- It can withstand improper or fraudulent employee behavior, IT infrastructure failures, disruptions of interdependent supply chains or customer channels, intellectual property theft, adverse economic conditions accross markets, and the myriad other discontinuities companies face today.

Establishing greater resilience is especially necessary in the current economic and security environment, which poses a new set of challenges to executives and boards. The openness and complexity of today's extended enterprise increases the firm's dependence on global financial, operational, and trade infrastructure. Although that provides for greater efficiency and effectiveness, it also exposes most companies to risks that were unfamiliar during the era of national markets and the vertically integrated enterprise – and compounds the effect of conventional business risks. What's more, the legal and regulatory landscape has undergone significant change since the September 11, 2001, terrorist attacks and the accounting and governance scandals in the United States, raising the level of diligence stakeholders expectation from senior executives, board of directors, and board audit committees in ensuring the safety and continuity of the enterprise. The July 2002 Unites States' National Strategy for Homeland Security recommends that industry sectors and corresponding government agencies responsible for critical infrastructure protection develop national infrastructure assurance plans that bridge the public and private sectors. The Sarbanes-Oxley Act of 2002 has tightened boards of directors's audit committee responsibilities, imposed new CEO and CFO certification requirements, and raised the "standard of care" obligations on management dramatically. The Basel II Accord commits financial-service institutions to set aside larger capital reserves against possible future operational disruptions. Guided by these and other requirements, underwriters of risk, such as insurance, equity and debt markets, will more aggresively distinguish between those businesses that are resilient and those that are not. To maintain earnings consistency and preserve and grow shareholder value, chief executives and board members need the capacity to sense and respond effectively to increasingly complicated levels of risk – risks that cannot necessarily be transferred through conventional means, such as insurance (Starr, Newfrock and Delurey, n.d.).

We are now living in an interdependent world. Traditionally, risks have not been perceived in the context of key earnings drivers, but rather in broad categories, each of which was managed in a functionally isolated way. Rarely do they or their business continuity programs link together in support of strategic objectives. Networks are one of the great advances in industrial organization. Over the course of the last half century, the vertically integrated company has given way to the networked enterprise, an organizational structure characterized by greater agility and adaptability. Successful firms today must deal with intertwined layers of information, raw materials, analytical data, customer communication and service and network infrastructure – at unprecedented speed – while maintaining countless secure relationships with third-party organizations, such as suppliers, technology outsources, and government regulators. The reliance on open borders, transnational alliances, and global markets for capital, goods, and services has generated a “just-in-time” economy, which, although remarkable cost-efficient, leaves companies open to a range of discontinuities that can affect operations, reputation, customer habits, legal standing, regulatory compliance, earnings performance, and ultimately shareholder value. We call these new vulnerabilities, collectively, interdependence risk, and define it as unanticipated risk exposure accross the extended enterprise that is beyond an individual organization’s direct control. The scale and impact of a disruptive event is a function of the degree of its integration into a broader extended enterprise. A problem that appears localized could ripple accross an extended enterprise, an industry sector or even a national or multinational economy. The capacity to withstand such disruptions is a function of a firm's systemic resilience – it's ability to understand its interdependencies and to foresee and plan around discontinuities that can occur within them (Starr, Newfrock and Delurey, n.d.).

Same opinion on interdependency is also noted by another author. As Richardson (1994) notes on human being living condition, our environment has become a more crowded world and as the population increases, pressures such as urbanisation, the extension of human settlement, and the greater use and dependence on technology have perhaps led to an increase in disasters and crises. The world is also becoming more interdependent and connected so that small-scale crises in one part of the world can have a significant impact on other parts of the world. (Ritchie, 2004)

Enterprise Resilience Planning begins with the identification of the greatest risks across the enterprise, including interdependencies, and then generates a targeted program, integrated with overall corporate strategy, for mitigating these risks. There are three steps to becoming a resilient enterprise :

- Diagnose enterprise-wide risk and interdepencies
- Adapt corporate strategy and operating model
- Endure increased risk and complexity

Disruptions are events that interrupts normal business, functions, operations or processes, whether anticipated or unanticipated (business continuity institute, 2011, p.16). A business interruption is something that disrupts the normal flow of business operations (Wallace and Webber, 2011). While disruption represents general circumstance of interruptions. A disaster is any event that disrupts a critical business function (Wallace and Webber, 2011).

Organizations may utilize tools such as Business Impact Analysis (BIA) to analyze business functions and effect that a business disruption might have upon them (Business Continuity Institute, 2011). It is also an explanatory review of the important functions that are essential for the operation of the business (Wallace and Webber, 2011).

Enterprise resilience is the ability and capacity to withstand systemic discontinuities and adapt to new risk environments (Starr, n.d.). It is an ability of an organization to resist being affected by an incident (Business Continuity Institute, 2011). Business continuity management is a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats – if realized – might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities (Business Continuity Institute, 2011).

Business continuity management main components that most discussed and as implied in the diagram are as below :

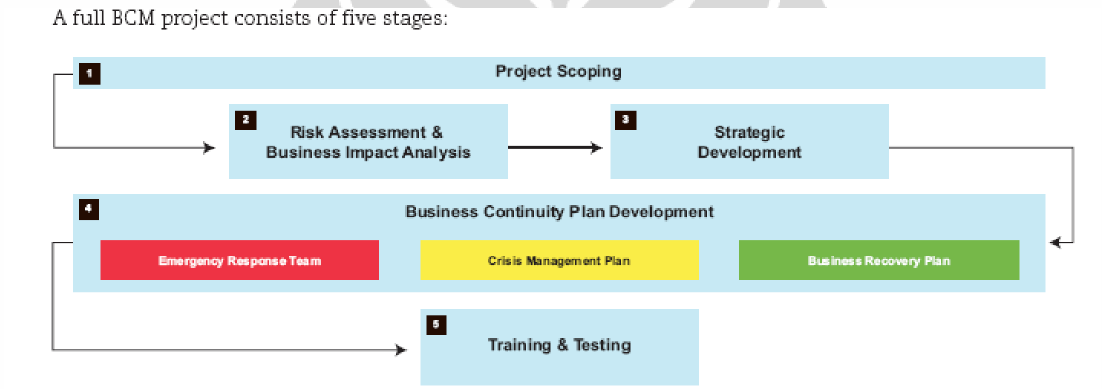

Figure 2.1 Business Continuity Management

Source : Internal documenation of PT XYZ and interview with Chief Operation Officer as in Appendix 1 with as edit as required

1. Emergency management

Emergency management provides a mechanism for implementing strategies aimed at reducing or eliminating risk and for building the capacity to protect the community from the unexpected (Choi, 2009).

2. Crisis Management

Crisis management is management of an incident needing a specialized and immediate respond, like dealing with a hostage situation, a major food recall program, etc. Crisis management is also called as incident management (Business Continuity Institute, 2011).

Faulkner (2001) argues that principal distinction between crisis and disaster are to the extent to which the situation is attributable to the organization itself or can be described as originated from outside the organization. Thus, a crisis describes a situation where the root cause of an event is, to some extent, self-inflicted through such problems as inept management structures and practices or a failure to adapt to change., while a disaster can be defined as where an enterprise is confronted with sudden unpredictable catasthropic changes over which it has little control (Ritchie, 2004). Heath (1998) believed that effective and well planned crisis management strategies were needed to prevent or limit the “ripple effect’ or outward chaos associated with crisis incidents not only between organizations but also across different industrial sectors (Ritchie, 2004).

3. Business Recovery Management

Business Recovery Management output is business recovery plan that is used to enable the organizations to resume all of its business processes within their maximum tolerable downtime.

The following diagram set forth interconnectedness between emergency management, crisis management and business recovery management during an incident/disaster.

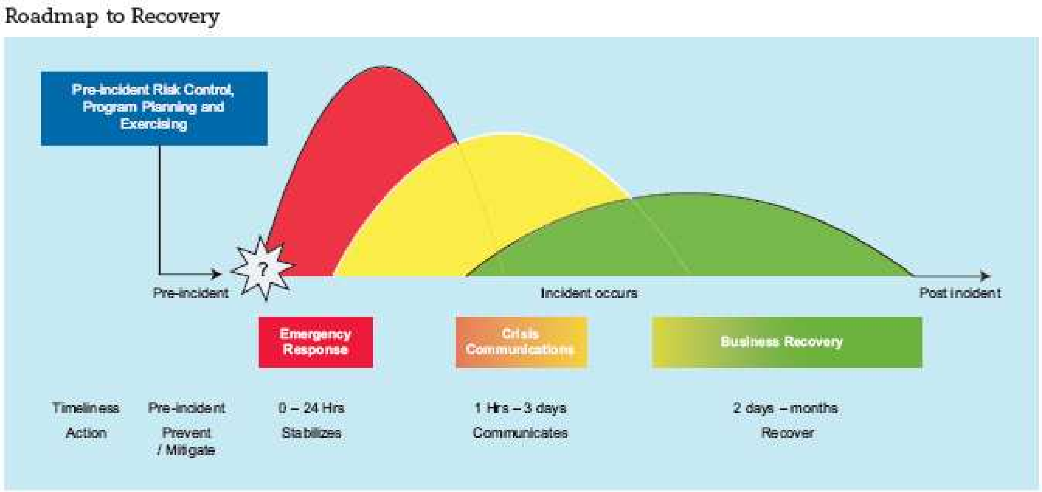

Figure 2.2 Interconnectedness of Emergency Management, Crisis Management and Business Recovery Management

Source : Internal documentation PT XYZ and interview with Chief Operation Officer with edit as required

Wallace and Webber (2011) and Business Continuity Institute (2011) state that disaster recovery management resides inside of a business continuity management which deals with strategies and plans for recovering and restoring the organizations technological infrastructure and capabilites after a serious interruption. Disaster recovery is now normally used as reference to recovery of an organization’s IT and telecommunications. Disaster Recovery Plan (DRP) that is further discussed in this thesis refer to the activities associated with the continuing availability and restoration of the IT infrastructure when a disaster(s) strike.

A recent research argued that disaster and crisis can do be avoided. Tinsley, Dillon and Madsen (2011) research reveals a pattern : Multiple near misses preceded (and foreshadowed) every disaster and business crisis they studied and most of the misses were ignored or misread. Two barriers to take lessons learnt from near misses:

a. Cognitive biases. Two in particular cloud people judgement:
    - Normalization of deviance that is the tendency over time to accept anomalies, particularly risky ones, as normal. For an organization, such normalization can be catasthropic.
    - Outcome bias

      When people observe successful outcomes, they tend to focus on the results more than on the (often unseen) complex processes that led to them.

b. Leaders tend not to grasp their significance.

Studies by Tinsley, Dillon and Madsen (2011) show that organizational disasters rarely have a single cause. Rather they are initiated by the unexpected interaction of multiple small, often seemingly unimportant, human errors, technological failures, or bad business decisions. These latent errors combine with enabling conditions to produce a significant failure. Near misses arise from the same preconditions, but in the absence of enabling conditons, they produce only small failures and thus go undetected or are ignored. It makes little sense to try to predict or control enabling conditions. Instead, companies should focus on identifying and fixing latent errors before circumstances allow them to create a crisis. The good news is near misses can be recognised and prevented by below seven strategies :

a. Heed high pressure

   The greater the pressure to meet performance goals such as tight schedules, cost or production targets, the more likely managers are to discount near-miss signals or misread them as signs of sound decision making. When people making decisions under pressure, psychological research shows they tend to rely on heuristics, or rules of thumb, and thus are more easily influenced by biases.

b. Learn from deviations

   Manager's response when some aspect of operations skew from the norm is often to recalibrate what they consider acceptable risk. Our research shows that in such cases, decision makers may clearly understand the statistical risk represented by deviation, but grow increasingly less concerned about it. Managers should seek out operational deviations from the norm and examine whether their reasons for tolerating the associated risk have merit.

c. Uncover root causes

   Correct the underlying cause not the symptom

d. Demand accountability

   Even when people are aware of near misses, they tend to downgrade their importance. One way to limit this is by requiring managers to justify their assessments of near misses.

e. Consider worst-case scenarios

   Unless advised to do so, people tend not to think through the possible negative consequences of near misses. Examining events closely helps people distinguish between near misses and successes and they'll often adjust their decision making accordingly.

f. Evaluate projects at every stage

When things go badly, managers commonly conduct postmortems to determine causes and prevent recurrences. When they go well, few do formal reviews of the success to capture its lessons. By critically examining projects while they're under way, teams avoid outcome bias and are more likely to see near misses for what they are.

g. Reward owning up

Seeing and attending to near misses requires organizational alertness, but no amount of attention will avert failure if people aren't motivated to expose near misses.

Fail to expose and correct latent errors even when the cost of doing it small, will lead to missed opportunities for organizational improvement before disaster strikes. Surfacing near misses and correcting root causes is one the soundest investments an organization can make.

2.2 Business Impact Analysis and Risk Assessments

Wallace and Webber (2011) defines Business impact analysis (BIA) as a snapshot of vital business functions at a given point in time. Any major changes in the operation of the business will require an update to BIA. An organization's critical functions depend on its primary mission. Benefits of BIA :

- Quantifying the tangible and qualifying the intangible costs of the loss of a critical function
- Identifying the most critical functions to protect
- Pinpointing the critical resources necessary for each function to operate such as people, equipment, software, etc.
- Determining the recovery time objective (RTO) of critical functions.
- Identifying vital records and the impact of their loss
- Prioritizing the use of scarce resources if multiple functions are affected at the same time.

Business impact analysis helps the Company to identify their critical business functions. Risk analysis is the next process that can be used to identify probable threats to our business functions (including the critical ones). Risk Assessment will then comparing the risk analysis to the controls that the company have in place to mitigate the risks in order to detect areas of vulnerability.

Business impact analysis, risk analysis and risk assessment are crucial piece of information in the Business Continuity puzzle which are the fundamental of any well-crafted disaster recovery plan.

2.3 Business Continuity Plan

Business continuity planning should be an integral part of every business, large and small, public and private, for-profit and non-profit. Every business should plan for how it would continue to operate in the face of interruption from a variety of natural or man-made hazards It may seem to be daunting, but business continuity planning doesn't have to be complex. At the basic level, the planning process follows a logical progression of steps (Association of Contingency Planners, 2011) :

1. Identify what hazards apply to your business. These can be natural hazards (e.g. severe weather, earthquakes, volcanic eruptions, etc.) or man-made hazards (e.g. computer viruses, vandalism, theft, etc.).
2. Determine the risk that these hazards pose to your business. Probability, severity and length of impact involving these hazards will help determine how much and what kind of risk each poses.
3. Develop plans and procedures to help your business prepare for, respond to and recover from interruptions. For example, you may determine that a power failure would cause you to lose access to your critical accounting records. You may implement a plan to provide backup power by purchasing a generator and ensure your records are backed up to tape or other media.
4. Continue to refine your plans through exercises and evaluation of how they performed in real events.

Types of Business Continuity Plan according to Wallace & Webber (2011):

2.3.1 Administrative Plan

The administrative plan contains or describes :

- How the company's business continuity program is conducted. It pulls together documents created during the initial program development such as BIA and risk assessment, into a single document for future reference.
- The company's long term strategy for contingency planning
- Set the expectations as to what each team member will be working on
- A valuable source of informations as it contains series of reference information common to all departments/programs scattered all around the department. During an emergency, it will be difficult to find all of this material.
- How the plans will be periodically tested in ever-increasing depth
- How the plans will keep pace with significant process changes
- How to maintain an ongoing employee awareness campaign

2.3.2 Technical Recovery Plan

This plan offer detailed instructions for how to re-create a technical function for a company. It can be for the recovery of anything vital to the business. In terms of the overall disaster recovery, only vital business functions are candidates for a technical recovery plan because the creation and maintanance of these plans is time consuming and expensive. The creation of recovery plans beyond the minimal, helps to raise a company's business resilience from disaster recovery to business continuity. A technical recovery plan provides a manager the tool to begin the recovery process while waiting for technical assistance to arrive. It covers :

- All vital IT functions, as identified by the Business Impact Analysis
- All vital business functions, as identified by the Business Impact Analysis

- Telephone service such as the main telephone switch, automatic voice mail routing, etc.
- Essential facilities services such as water, electric, sanitary, etc
- The office operations of vital business functions

2.3.3 Work Area Recovery Plan

Work area recovery means preparing workspace to temporarily support recovery of business operations. Some companies overlook the fact that recovered IT operations are of little value if the other part of operations (work area) are not recovered as well. Challenges in writing this plans are :

2.3.3.1 Selecting a Recovery Site

Table 2.1 Selecting a Recovery Site

	Security	Inbound Telecom	Data Bandwith	Time to Activate	Potential Problems	Relative Cost
Different company site	Total control	Control over capacity	Known	Minimal, a few hours if properly equipped	Clearing out whoever is using the equipment	Expensive, unless the facility is used for low value uses
Contracted hot site	High	Available capacity	Available capacity	24 hours	Nearest available site may be far away	High
Mobile recovery equipment	Your responsibility: total control but perimeter is open	Limited to equipment capability	Limited to equipment capability	24 hours	If the company site is unavailable, must find another quickly	High

Table 2.1 Selecting a Recovery Site (Continued)

	Security	Inbound Telecom	Data Bandwith	Time to Activate	Potential Problems	Relative Cost
Scramble at the time of incident	Multiple sites mean minimal control	Too dispersed to easily swing the inbound calls to a site	Dispersal should provide adequate bandwidth to each site	Long; this is an untested plan	Recovery delayed while locating a site, which may require preparation	Zero until it is needed and then high

Source : Wallace & Webber (2011)

2.3.3.2 Employee Notification

Immediately after a disaster is declared or an incident activates a business continuity plan, the recovery facility crew is notified. It is suggested that this crew is notified by company's automated notification system. Alternatively, a call tree may be used.

2.3.3.3 Tools to Work With

A personal computer with a network connection and a telephone are the primary tools provided to an office worker. Work together to develop a standard workstation layout. This will ease unit setup and IT support. Other tools needed are printers, reference materials detailing the recovery facility.

2.3.3.4 Telecommunications and Data Systems

A recovery site must have a data connection to the recovered IT site. The bandwidth must adequate to support workstations at site. Moving the inbound call lines from the damaged work site to the recovery location.

2.3.3.5 Security

The recovery site requires both physical security to protect assets and information security to protect its data.

Before a work area recovery plan can be declared as operational, it must be :

a. Tested. The ideal plan must demonstrate that it able to meet the recovery time objective (RTO) designed during the planning phase.

b. Maintained. The recovery site will require a regular maintenance periodically.

2.3.4 Pandemic Management Plan

Pandemic plan is subpart of business continuity planning. A pandemic refers to an infectious disease that is spread by contact with people, strikes a significant portion of a population over a wide area, often over continents. Pandemic slowly appears, overwhelms the population and then gradually recedes.

Pandemic Techniques must be included in the plan are :

2.3.4.1 Social Distancing

Infectious disease is spread by person-to-person contact. The farther apart people are, the less likely it is that they can pass germs to others. Pandemics require loosening the company’s absence policy to ensure sick people stay home.

2.3.4.2 Sanitation and Immunization

People touch many things. Thus things around the office must be properly cleaned at least daily to reduce the passing of germs through touch. Arrange paid immunization for employees and their families to reduce sick time absences, reduce likelihood of an employee infection and increase employee participation.

2.3.4.3 Communications

Keep the workforce and the public informed about the pandemic, explaining the symptoms, what each individual should do and what the company is doing about it. Communication plans must be in place before they are needed so that everyone knows where to look for what they need.

2.3.4.4 Timing

Know when to activate your pandemic plan and when to close it down.

2.3.4.5 Use Technology

Use technology to enable people to work from home and stay separated from potential infection.

2.4 Disaster Recovery Plan as part of IT Technical Recovery Plan

2.4.1 Business Continuity Plan vs Disaster Recovery Plan

Wallace and Webber (2011) tries to interrelates between Business Continuity Planning and Disaster Recovery Planning. Business continuity addresses continuing a company's business after an adverse event. Historically disaster recovery was the term for rebuilding the data center at another site after the existing one has been rendered unusable. Disaster recovery will solved the problem of a total data center loss but the real issue is the overall business processes of which automated systems are just one part of it. Nevertheless, disaster recovery planning is still important for both the data center and the offices. It resides inside of a business continuity plan which deals with the overall issue of keeping the business running (p. 115).

BCM aims to proactively manage all business processes, assets, facilities, supply chains and human resources to ensure that the business will function at its highest capacity. This is distinct from disaster recovery-based planning which concentrates on ensuring that IT contingency plans and procedures are in place to return to business as usual as soon as possible after a crisis. BCM sees disaster recovery as a sub category.

As stated by Miller (2011) in the www.continuitycentral.com, BS 25777 emphasises that IT Disaster Recovery is simply one aspect of IT continuity which has to be viewed in the same holistic manner as wider business continuity management. It is BCM which seeks to ensure that the organizational processes are protected from disruption and that it can respond positively and effectively when disruption occurs. BS 25777 is developed by the BS 25999 committee, the committee under British Standards Institution who creates standard for business continuity management.

2.4.2 Disaster Recovery Planning

Reddick's research (2011) shows that there has been a significant impact of IT usage in state governments on emergency planning. IT has been proven to be effective for all phases of emergency management, especially for the response phase. It was evident that state governments rating high on a performance index were more likely to use IT for emergency management.

According to Pine (2007) there are numerous important technologies that are used in emergency management. Rao et al., (2007) mentioned they are seven that are universal. They are the internet, wireless technology, GIS, direct and remote sensing, emergency management decision support system, hazard analysis and modelling, and warning systems. Nikolic et al. (2007) states that they can be combined in a multimedia platform for creating an overall emergency management information system (Reddick, 2011).

National Governor's Association (NGA) in 1979 was the first to develop a broad framework for emergency management during its study of emergency preparedness. These functions have been examined to demonstrate the impact of IT on emergency management. NGA identified four phases of emergency management Below are the emergency functions/phase that combining IT role in disaster recovery management within the context of strategic management framework (Reddick, 2011; Choi, 2009; Foster and Dye, 2005; Ritchie, 2004) :

Pre-event stage allowing the development of strategy and plans:

- Hazard Mitigation / Prevention

  Risk assessment of current condition followed with collaboration with senior management to develop plan for reducing risks. In DRP-IT context, these are the information technology activities that are undertaken in the long term before the disaster actually strikes. They are designed to prevent emergencies and reduce the damage resulting from those that occur.

Pre-event stage with continued implementation of strategies to control or reduce the severity of the crisis/disaster.

- Disaster Preparedness

  Contingency planning by collaborating with business units to develop "what- if" scenarios for loss of critical infrastructure and telecommunications, including alternative facilities and service provider contracts. Also develop workplace strategies to develop alternative officing strategies that meet business continuity goals. In DRP-IT context, these are the information technology activities undertaken in the shorter term, before the disaster strikes, which enhance the readiness of organizations and communities to respond to disasters. The following graph illustrates the impact of having a preparation in respect to negative impact, speed recovery and business advantage.

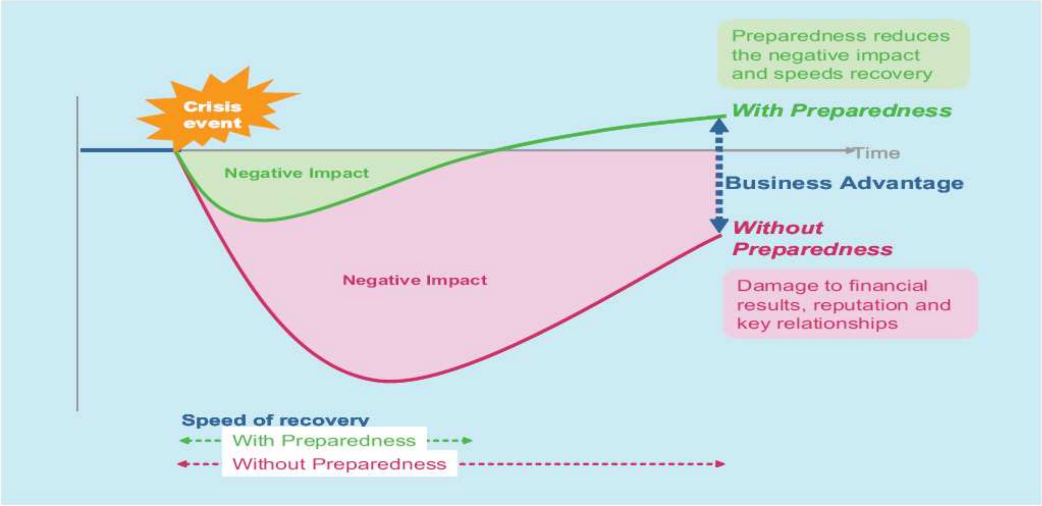

Figure 2.3 The Effect Of Preparation To Negative Impact, Speed Recovery And Business Advantage

During event stage is a stage immediately before or after a crisis or a disaster occurs which requires the implementation of strategies to deal with its impacts :

- Disaster Response Activities

  Develop roles for employees integrating with the corporate crisis management team. In DRP-IT context, these are the information technology activities undertaken immediately following a disaster to provide emergency assistance to those in need and minimize property damage, such as emergency plan activation, activation of emergency systems, emergency medical assistance, shelter and evacuation, and research and rescue.

Post event stage is the phase in which a long-term recovery or resolution phase allowing for evaluation and feedback into future prevention and planning strategies for destinations and businesses :

- Disaster Recovery Activities

  Contingency plan implementation and restoration strategy. In DRP-IT context, These are the short-term and long-term information technology activities undertaken after a disaster to provide victims in an affected area with at least their pre-disaster condition of well being.

2.4.3 IT Recovery Strategy

Based on Wallace & Webber (2011), IT recovery steps include rebuilding :

- Environmental

  IT equipment must stay within a specific temperature and humidity range.

- Infrastructure

  External network connection into the data centre of the local service provider and throughout the recovered data centre; critical servers used by application servers such as domain controller, DNS, DHCP, etc. Architecture diagram could help better visualise and faster understanding.

- Applications

  Company specific software used by the business to address customer and internal administrative requirements. The detailed applications :

  - Prerequisite systems/applications that are required prior to restoring this application
  - Successor systems/applications that are fed by this application
  - Application or infrastructure component license requirements

- Data

  The information needed by the company’s business departments to support the flow of products and services.

2.4.4 Data Recovery Strategy

Based on Wallace & Webber (2011), There are 2 types of risks in the infrastructure that supports your data assets :

a. Physical loss due to a device failure or disaster at your location.

Physical loss is the likely of the two but it is potentially the most damaging. It includes hard disk failure, server failure, or an enviromental disaster. Physical loss accounts for 20% of all incidents affecting information technology resources.

b. Logical loss caused by an application or user error

It includes application errors, user errors or a security breach. Logical loss account for approximately 80% of all incidents.

2.4.4.1 Based on Wallace & Webber (2011), in assessing risk, considerations for Key Causes of Data Loss :

- Viruses

  These malicious program can get into your system at any time and strike when you least expect it.

- Natural disasters

  Fire, flood and high winds can cause physical damage to systems and make your data unavailable or unreadable

- Human-created outages

  Systems can be damaged by a sudden loss of power, or worse yet, a small part of data stream can be lost, causing damage that may not be readily apparent.

- Hard drive crash

  It's not if a hard-drive will fail, but when. A hard drive is most likely to fail within 90 days of being placed in service and after about three years of average us

- Laptop or smartphone loss or theft

  The value of the data stored in a laptop or other portable device usually far exceeds the cost of replacing the hardware.

- Software failures

  Operating systems and storage area network software can fail, corrupting existing data

- Application failures

  Applications are not guaranteed to be bug free. A bug in an application can cause incomplete or incorrectly formatted or calculated data to be written into your files.

- Vendor failure

  Your data could be at risk if the vendor suddenly out of business or no longer able to provide the required services due to certain limitations.

  There are tactical and strategic issues surrounding the loss of critical corporate information :

  a. Tactical issues
     - Compromised information
     - Lost productivity
     - Employee downtime
     - Loss of customer information
     - Increased help desk support required

  b. Strategic issues
     - Loss of opportunity
     - Decreased operational efficiency
     - Inability to support customers
     - Increased system costs
     - Noncompliance issues

  c. Other issues
     - Customer notification
     - Litigation expenses
     - Internal investigations
     - Forensic experts
     - Software updates
     - Subpoenas by government authorities
     - Stock price
     - Reputation

CHAPTER 3
METHODOLOGY

This chapter explains methodology being used in a step by step format starting from research design to data analysis as basis to address problem as outlined in chapter 1.

3.1 Research Method

This thesis use a descriptive qualitative research method. This will include examining factors that might influencing behaviors, environments, circumstances of a subject in a descriptive way. Descriptive research may focus on particular subjects and go into great depth and detail in describing them. This approach is called a case-study. Case studies identify and provide evidence to support the fact that certain parts/variables exist and that they have construct validity. Therefore the important aspect of this method is how to collect experience, opinion, feeling, and the knowledge from the participants and afterwards adapting it to the aforementioned disciplines (Patton, 1990).

3.2 Research Stages

3.2.1 Data Collection

The research is initiated with data collection process of both primary and secondary data. Primary data is the type of data that is obtained directly and usually never been published before. The sources of primary data is through interview and direct observation. Secondary data is the type of data that is obtained by other party and already published before. The sources of secondary data is organizations data, government/regulatory website, books, journals, magazine, newspapers, etc. Data collection process for this thesis is done through:

- Secondary data - Literature studies with subjects being discussed mostly are risk management, enterprise risk management, business continuity management, business resilience and disaster recovery management.
- Primary data - Field observation of current situation in PT. XYZ

- Primary data - Interview with the Chief Operation Officer and IT Dept. Head of PT. XYZ
- Secondary data - Data acquired from PT. XYZ's management (e.g. company's intranet)

3.2.2 Data Analysis Risk Assessment

Data analysis that related to PT. XYZ's risk identification and risk assessment. The purpose is to understand the underlying risks currently faced by PT. XYZ particularly their critical business risks as not all business risks were visible to be addressed. Risk identification and assessment will help the management to understand the challenge they need to overcome and to ensure sufficiency of their internal control to mitigate such risks. Data acquired are both primary and secondary data. Primary data is obtained through interviews to identify the risks and direct observation. Secondary data is obtained from PT XYZ's management (i.e PT XYZ's intranet). PT. XYZ maintain a risk register/risk profile (listing of risks they perceived to have a significant business impact).

3.2.3 Data Analysis Theoretical Framework

Data analysis related to company's business disaster recovery plan. The analysis will use 2 frameworks provided study literature in chapter 2 refer to point 2.4.2 – 2.4.4:

- Emergency functions/phase that combining IT role in disaster recovery management within the context of strategic management framework (Reddick, 2011; Choi, 2009; Foster and Dye, 2005;Ritchie, 2004). We tried to analyze management's response to any disaster based on their available disaster recovery plan to assess their preparedness using such 3-time-phase framework (Pre-event, During and Post-event stage).
- Recommended IT Recovery Strategy including infrastructure, applications, and data management (Wallace and Webber, 2011).

3.2.4 Conclusions and Recommendations

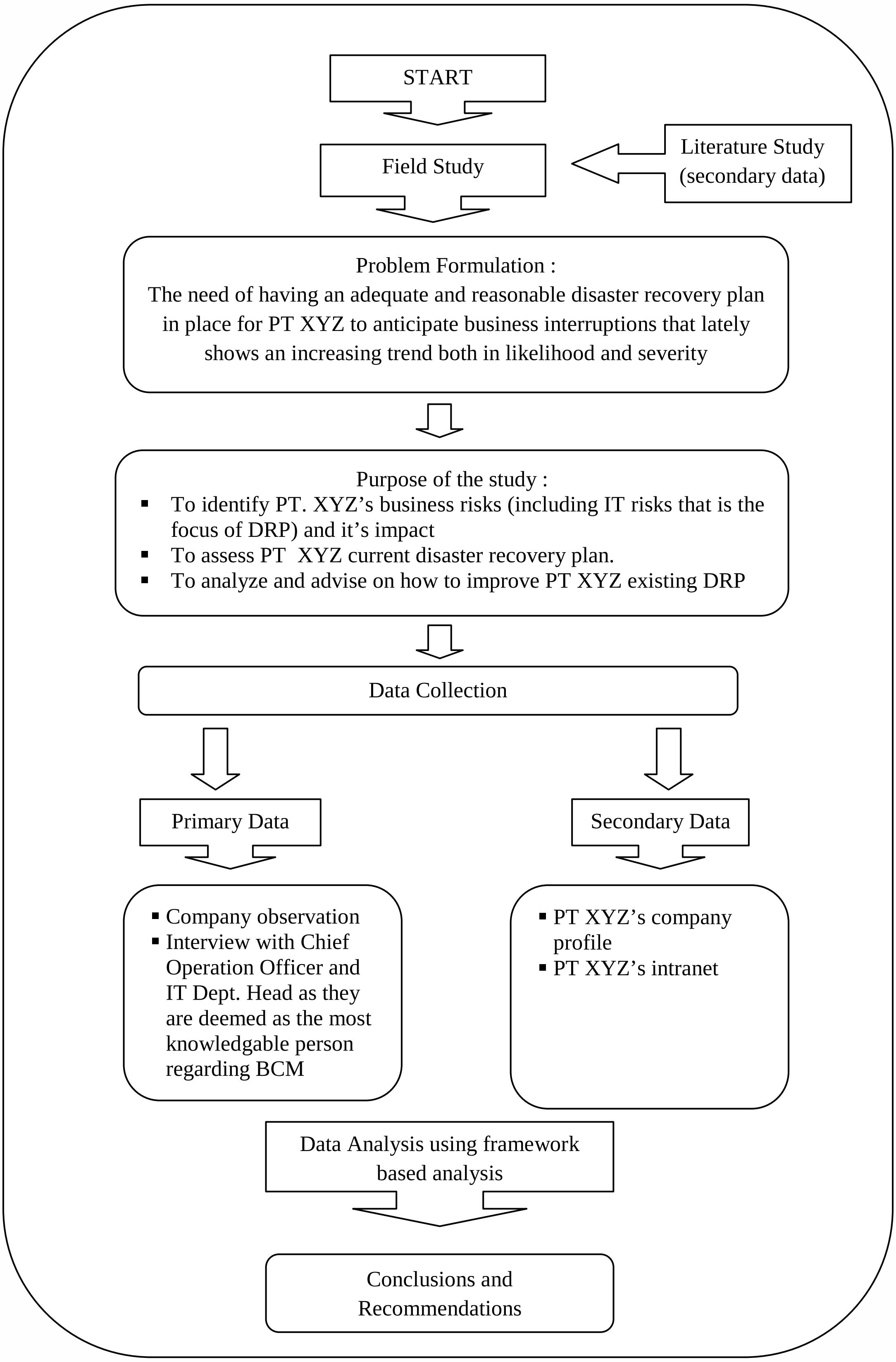
START
Field Study
Literature Study (secondary data)
Problem Formulation :
The need of having an adequate and reasonable disaster recovery plan in place for PT XYZ to anticipate business interruptions that lately shows an increasing trend both in likelihood and severity
Purpose of the study :
▪ To identify PT. XYZ's business risks (including IT risks that is the focus of DRP) and it's impact
▪ To assess PT XYZ current disaster recovery plan.
▪ To analyze and advise on how to improve PT XYZ existing DRP
Data Collection
Primary Data
Secondary Data
▪ Company observation
▪ Interview with Chief Operation Officer and IT Dept. Head as they are deemed as the most knowledgable person regarding BCM
▪ PT XYZ's company profile
▪ PT XYZ's intranet
Data Analysis using framework based analysis
Conclusions and Recommendations

Figure 3.1 Research Methodology Steps

CHAPTER 4
ANALYSIS

4.1 The Company's Establishment and Business Background

4.1.1 The Company's Establishment

PT. XYZ is a one of the local subsidiary of global professional services firm providing advice and solutions in the area of risk and insurance services specifically :

- Insurance broking and services.

  PT XYZ employs a team approach to address clients' risk management and insurance needs. Each clients relationship is coordinated by a client executive who draws from the many industry and risk specialities within PT XYZ to assemble the resources needed to analyze, measure and assist a client in managing its various risks. Product and service offerings include program design and placement, post-placement program support and administration, claims advocacy, and wide array of risk analysis and risk management consulting services. Its specialties including Aviation & Aerospace, Claims, Energy, Infrastructure and Marine areas.

- Risk management activities (risk advice, risk transfer, risk control and mitigation solutions).

  Comprised of consulting specialists dedicated to providing clients with advice and solutions across a comprehensive range of insurable and non-insurable risk issues. It helps clients identify exposures, assess critical business functions and evaluate existing risk treatment practices and strategies.

PT XYZ's clients vary by size, industry, geography and risk exposures. PT XYZ is organized to serve clients efficiently and effectively, delivering tailored solutions based on complexity of the risk and global footprint, and matched to clients' buying styles.

PT. XYZ was established in 1999 as a result of consolidation performed by PT XYZ's current ultimate parent with 2 acquired multinational companies (a claim management services company and an international insurance brokerage firm). Since its first establishment in Indonesia, PT. XYZ utilized IT devices and built the related IT infrastructure to support daily business services. PT. XYZ's IT framework followed the know-how IT arrangement from its parent company.

4.1.2 Vision and IT Operating Principle

PT. XYZ's vision is to be the number one choice in every market we serve. One of PT. XYZ's operating principle is that it develop and deploy systems that enhance client service, internal productivity and market interactions. This clearly implies company's recognition on the importance of IT usage in their operation.

4.1.3 Indonesian Insurance Business Environment

The Indonesian insurance industry is controlled and regulated by the Directorate of Insurance, a division of the Ministry of Finance. The Indonesian (non-life) insurance markets should be considered as a developing financial services sector in the emerging Indonesian economy. With a few notable exceptions, Indonesian insurance companies are now subject to having minimum Paid-Up Capital requirements (IDR 40 b by 2010 end, IDR 70b by 2012 end, IDR 100b by 2014 end) and continuing to develop and strengthen its technical and professional skills to be in line with today's developed industrial countries. As at 1 January 2009, there were 88 registered Property and Casualty insurance companies, 43 registered Life insurance companies, about 145 registered insurance brokers plus hundreds of insurance agents. Of these total insurers and brokers, there are 16 international insurers and 4 international insurance brokers licensed in Indonesia, including PT. XYZ

4.2 PT.XYZ's Risk Management Policy

The risk management policy obtained from and discussed with Chief Operation Office (refer to Appendix 2) states what must be done with respect to risk management and the responsibilities of certain groups and individuals in respect to risk.

4.2.1 Definition of Risk

Risk for PT. XYZ can be defined as “the possibility of an event occurring that will have an impact on the achievement of the firm’s objectives. The inherent risks facing the firm can be categorized into eight risk categories. They are :

- Compliance/regulatory
- Business processing
- People
- External
- IT Systems / Infrastructure
- Financial
- Clients products and markets
- Strategic

4.2.2 Objective of Risk Management

Objectives of risk management and the internal risk assessment framework include :

- Protect our margin and help us to grow faster with confidence
- Protect our clients and shareholders
- Prevent us inadvertently breaking the law
- Avoid reputational damage
- Help support parent credit rating
- Provide confidence to our business partners
- Avoid any sanctions

Therefore any potential event that can threaten the Firm’s objectives (including compliance with applicable laws and regulations) should be considered within the definition of risk and the internal risk assessment framework.

4.2.3 Responsibilities for the Management of Risk

Responsibilities for the management of risk are inherent in all roles throughout organization, from senior level to every member of staff.

a. Risk governance committees (i.e Executive Committees/Excom).
   Excom is the ultimate governance body responsible for the management of the firm and is therefore ultimately responsible to manage risk.

b. Responsibilities of every colleague. The risk responsibilities of every colleague include :
   - Undertake their activities in a risk conscious manner
   - To be aware of and manage on an ongoing basis any risks relevant to their role and immediate working environment
   - To report any material risk issues that they are aware of to their supervisors

c. Responsibilities of Business Units/Support Areas
   The management of each business unit hold the primary responsibility for the management of risk within their own areas of coverage, including :
   - To identify key risks facing their areas of accountability
   - To regularly assess their effectiveness at identifying and managing these risks on an ongoing basis
   - Where there is a “hand-off” risk between two areas each area is responsible to ensure that the associated risks are properly managed.
   - To respond to material risk incidents/issues as they occur and take appropriate action to mitigate / escalate, and in accordance with any relevant policies
   - To escalate any material risk issues to the relevant functional management as appropriate
   - Promote and encourage a risk aware culture

d. Responsibilities of Risk and Control Functions
   PT. XYZ operates a ‘Lines of Defence’ model that aims to provide control, oversight and review across 3 distinct ‘lines’ :

Table 4.1 Risk Responsibilities and Control Functions in PT. XYZ

First Line	Business Units and support departments (e.g. Operations, IT, Finance)	Business and support functions are primarily responsible for the indentification and management of the risks associated with their business/activities
Second Line	Risk control functions e.g. Compliance, Legal, CRO Function	Control functions assist the business in the management of some specific risks especially where some specific expertize is required (e.g. lehal), and provide assurance over the management of risk in the first line
Third Line	Regional internal audit	Independent assurance over the effective operation of the first two lines of defence

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

The second line of defence is made up of individuals departments, such as HR, Compliance & Legal who, through their specialism :

- Assist the business to manage their specialist risks e.g. legal
- Challenge the business where risks have not been identified/or require improved assessment
- Provide an aggregated view of all similar risks across the firm paying particular attention to consistency

The third line of defence provides an independence assurance over the business and control function activities.

4.2.4 Overview of Risk Management Framework

The Internal Risk Management Framework is a coherent set of processes, which are designed to ensure the firm identifies, assesses, mitigates and manages its risks. The Framework consists of three layers:

1) Risk strategy & culture
2) Decision making/Risk Governance
3) Day to day risk processes

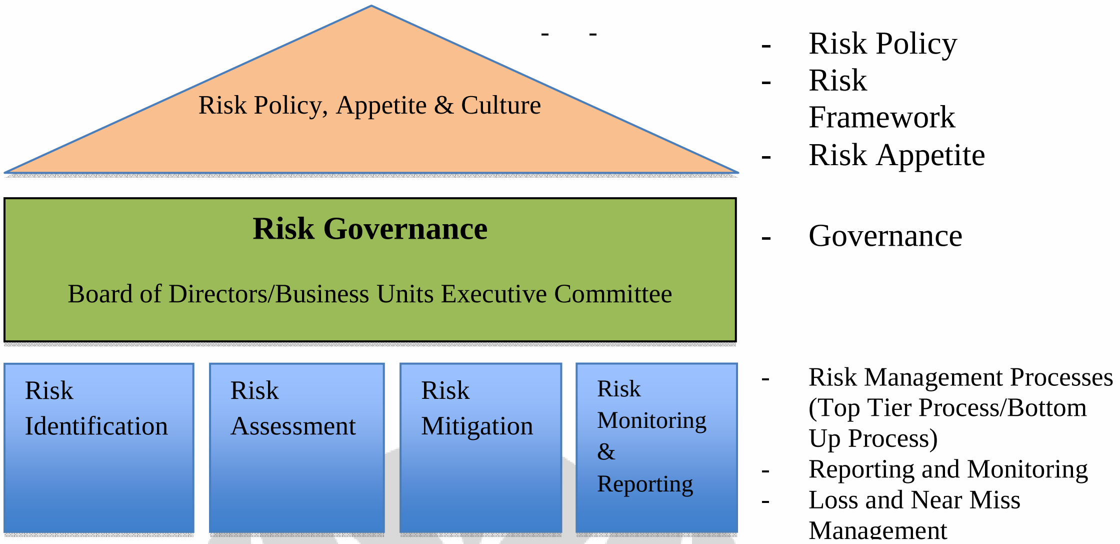
Risk Policy, Appetite & Culture
Risk Governance
Board of Directors/Business Units Executive Committee
Risk Identification
Risk Assessment
Risk Mitigation
Risk Monitoring & Reporting
- Risk Policy
- Risk Framework
- Risk Appetite
- Governance
- Risk Management Processes (Top Tier Process/Bottom Up Process)
- Reporting and Monitoring
- Loss and Near Miss Management

Figure 4.1 Internal Risk Management Framework

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

The day to day processes for risk management are supported by an established goverance structure, facilitating the flow of risk information from the Business Units team, up through to Business Units Executive Committee.

4.2.5 Risk Governance Process

The risk governance structure within the company is in place to provide a strong foundation for the management of risk across the organisation. Irrelevant of size and make up of the business unit, the flexibility of the framework supports the activity of risk management as well as the delegation / escalation of key risk issues.

Key Elements of Risk Management Governance in PT. XYZ

Business Unit Executive Group

Each business unit has management structures and governance meetings in place to manage their business. Risk information is escalated to these groups and reviewed / challenged. These allow for senior management review within the department and the ability to delegate to appropriate personnel for action within the business unit or escalate to higher risk governor for further action.

Business Unit Risk Register

Each business unit have a risk register. This is a standard template, to capture and document risk. It is used as an audit trail, action log and reporting mechanism.

4.2.6 Risk Processes

As stated in the company's risk policy and confirmed during interview with the Chief Operation Officer, the Risk Management process in PT XYZ involves two connected activities both following a continuous process of identification, assessment, mitigation and monitoring of risk informed by the Risk Appetite Statement.

4.2.6.1 Risk Identification.

The 'Top down' process and the 'Bottom Up' process work together in ensuring that risks are identified and managed at all levels of the organization :

- **Top Down -** Executive Committee regularly identify and review the 'Top Tier Risks' impacting the organization. Information from the business unit risk registers helps to highlight risks 'bubbling up' as well as validating the top down information. The ongoing review of these risks also includes validation from external sources such as industry information and external consultants.
- **Bottom Up -** The bottom layer of the framework consists of a number of "day-to-day" risk processes, although it should be recognised that some of these processes are not actually performed on a daily basis. See below for a diagram of how these components interact. The business units continually identify and review risks, maintaining a risk register using information from:
  - Standard business activity
  - Top Tier Risks
  - External Information
  - Change initiatives etc.

The keys stages of the process are:

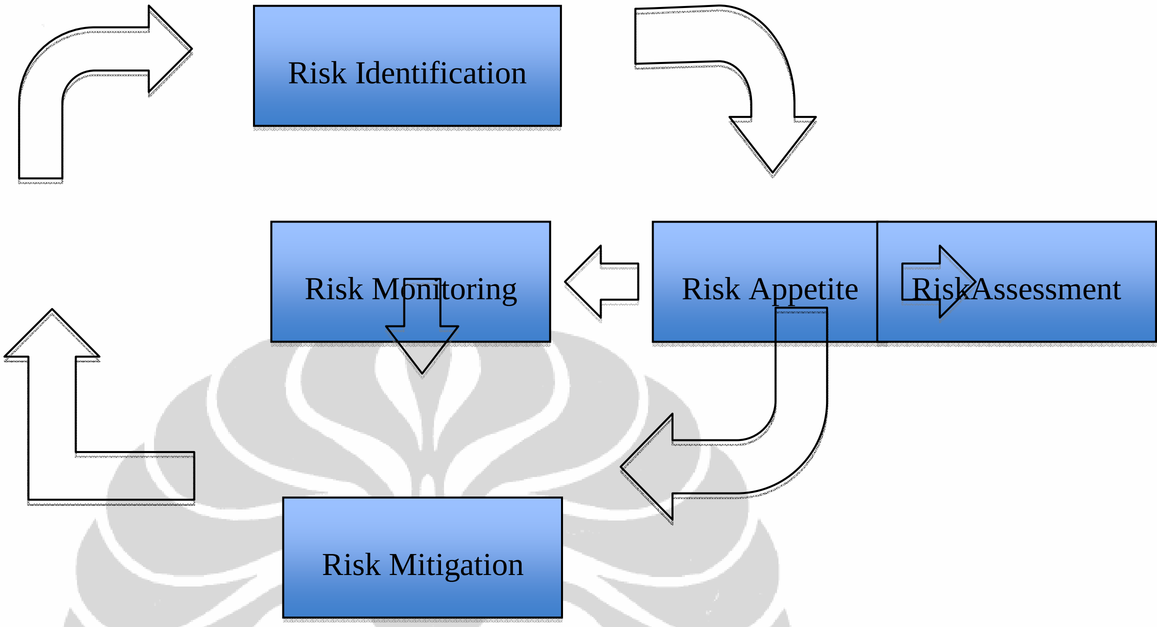

Figure 4.2 The Risk Process

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

The key aim of the risk identification phase is for the business unit to understand the threats to its objectives and what could prevent them from delivering their plans. Within specific activities such as Project Management and Business Planning, risk management is an embedded in the activity, and a key part in structuring the activity. It often forms part of the documentation from these activities and is an explicit output. Although all colleagues will identify risk as part of their normal day to day activity, this phase ensures the key risk information is captured in the Business Units risk register.

Risk identification should be embedded into standard business activity to ensure ongoing and regular identification of risk. This could include:

- At the start of project or initiative (and updated throughout its duration)
- As part of quarterly business reporting
- As part of the business planning and review

- As part of standard monthly business review and reporting

Use of the Risk Categories also helps to understand the full scope of risks the BU may face and assess the current coverage against it. Other risks could be identified via:

- Risks escalated by colleagues through their normal day to day escalation and supervision processes
- Risks already known by senior management in the area and part of their day to day management of the area
- Risks escalated directly from colleagues to the COO or other risk group attendees
- Risks identified from Top Tier report

As part of the consideration of the risks for the risk register, the Top Tier risks should be considered to determine whether they also impact the area in question. If so, and considered sufficiently material, these should be included in the Risk Register, even if contained in the Top-Down information.

The Risk Register

Within all Business Units a risk register exists to capture and evidence the risk management activity. It is critical that all key risks within the business are captured within the risk register, to allow structured review, challenge and escalation. The standard risk register template is created and owned by the COO (Chief Operation Officer) and is a simple Microsoft Excel spreadsheet. It provides structure to allow all key (BU top tier risks) to be documented as well as other, smaller risks (secondary risk) as well as allowing to maintain an audit trail of historical risks within the area (Removed risks).

4.2.6.2 Risk Assessment

Once the risks have been identified, they then need to be assessed to understand the impact they could have on the firm. In practical terms, an initial assessment will be carried out as the risk is identified to understand if it is a material / key risk.

In assessing any risk, the company take into account any historical loss data or experience to rationalise any score. They should also take into account both the likelihood AND the impact when settling on a score, not necessarily settling on a ‘doomsday’ scenario but a more credible evaluation for a risk.

A good example of this is risk associated with failure to adhere to regulation. Ultimately it is possible to be actually ‘shut down’ by the regulator and authorisation removed, but this scenario is unlikely to come about without a whole series of steps / issues occurring first, with plenty of opportunity to contain / remediate the problem. It is more ‘credible’ that we could be instructed to do a skilled person review and be fined. Still a very significant risk but not so impactful as being totally closed.

4.2.6.3 Risk Mitigation

Once a risk has been identified and assessed and a full understanding of the risk has been made, it is key to define the most appropriate course of action. Firstly, any risks above the risk appetite of the BU need mitigating action to be defined. Although, in some extreme circumstances, there may be some risks that we have to accept, by default we should aim to mitigate ALL risks in this area. The risk register supports the approach in which the risks are mitigated by prompting you to focus the action on:

- Reducing the Likelihood – Preventing it happening so frequently
- Reducing the Impact – Preventing the cost of it happening should it occur
- Reduce both – define a course of action that will tackle both elements
- No action – Accept that no action can be put in place at present (because it is too costly or the risk is at an acceptable level)
- Action dependant on another area – No action can be taken by the BU directly but action could be put in place by another areas, for example IT.

Once a focus for the action has been decided upon, the BU must decide on what actually needs to be done. Risk action should take one of the following 4 key forms:

1. Mitigate – identification of additional mitigating actions
2. Avoid – decide to avoid risk, e.g by ceasing activity

3. Transfer – e.g purchase additional insurance
4. Accept – recognise that the risk is higher than appetite, but monitor situation

4.2.6.4 Risk Monitoring

The monitoring and reporting of risk is a key activity in the cycle to keep track of progress on action, factors impacting the risk, external factors that may impact the risk and provide confidence of an improving risk profile. The key audience for risk information is the Executive / Management Meeting. This is where the risk information is 'integrated' with the other business information to support senior management. The key outputs from the 'bottom up' risk process is the risk register. Pulling together all information of this type from across the business units to analyse how the risks look if aggregated / occur at the same time.

There is no single manner on how to monitor each risk due to the differing nature of risks (eg monitoring external regulatory threats requires different monitoring to the level of E&O (Error and Omission exposure)). As part of the risk assessment process, there will be a consideration of any metrics to measure or monitor the risk.

4.2.7 Risk Appetite

PT. XYZ's level of income, balance sheet and risk appetite are all inextricably linked. PT. XYZ's risk appetite is a balance between the amount of profit it wishes to earn against the risk it is prepared to take to earn it e.g more risky investments need to earn more because the probability of the investment failing is higher or an insurer will want a higher premium for a risk that is more likely to occur (such as insuring properties on flood planes). The balance between increasing appetite in return for increased profit (or NOI) can be simplistically represented by the following diagram :

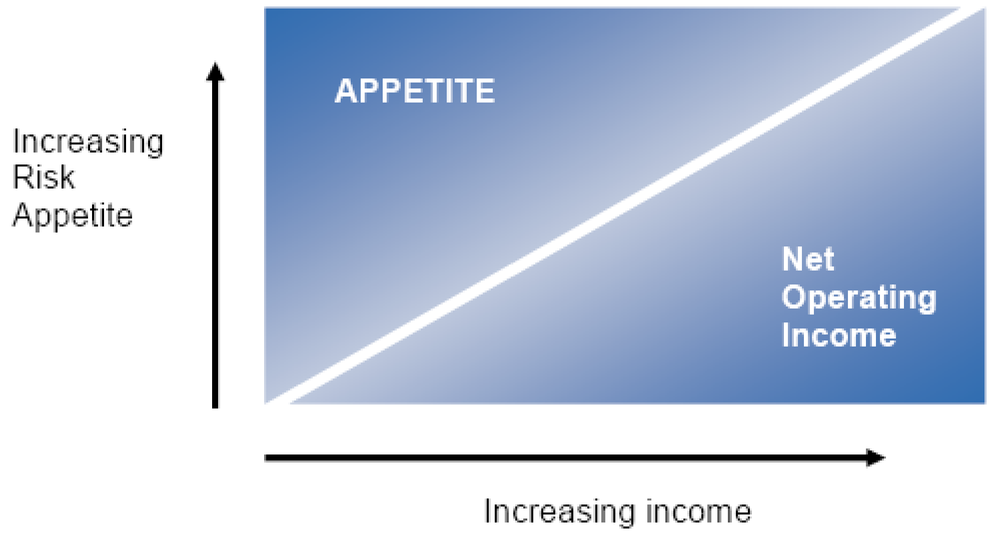

Figure 4.3 Risk Appetite Continuum

Source : PT XYZ’s internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

Each firm will have to set its’ own risk appetite as it is a function of the type of business they are in, geographic locations they trade in, product sets they deal in and ultimately its culture. Once established its level of risk appetite, it will need to articulate how that translates into daily activities and decision making. Thus, define level of tolerance toward specific risks.

Risk appetite levels have been set for each risk category explained in 4.2.1 :

Table 4. 2 Risk Appetite Rating

		Risk Appetite		
		Low	Moderate	High
Areas of Risk	Compliance & Legal	▨		
	Business Processing		▨	
	People		▨	
	External		▨	
	IT Systems / Infrastructure		▨	
	Financial	▨		
	Clients, Products and Markets	▨		
	Strategic		▨	

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

Risk appetite rating explanation :

Table 4. 3 Risk Appetite Rating Explanation

Risk Appetite	Description
Low	Is very risk averse in most circumstances
Moderate	Is willing to accept and actively seek some risks in certain circumstances
High	Is willing to accept risks in most circumstances

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

4.2.8 Loss / Near Miss Management

The objective of developing the structure and governance around the management of losses / near misses are:

- Through the central organisation and analysis of loss information prevent and or reduce the occurrence and impact of negative events in the future
- To provide a central repository for all loss / near miss information, a full cross section of risks and support root cause analysis
- To improve awareness of losses / near misses and the processes around their management

Risk Management is focused on the understanding, control and governance around business activity to prevent and / or reduce the occurrence of negative events. However, at times, these events do occur (i.e. a risk crystallises) no matter what mitigating activity is delivered. This can result in an actual loss or, through good fortune, good judgment or further action (or a little bit of each), a 'near miss'. It is critical that, as an organisation, we understand as much as we can about these events and use this knowledge to prevent, or at least reduce, the likelihood and scale of similar risks going forward.

Processes and a central repository for the management of these ''loss events' will help to collate and provide information to allow analysis of these events. The process has the following key elements:

1. Identification of loss / near miss
2. Communication of loss / near miss
3. Documenting of loss / near miss
4. Root Cause Analysis
5. Creation of action plan
6. Review and monitoring of activity

The process to collect information of losses / near misses is split into incidents giving rise to a potential E&O claim, and those that do not. This is to reflect the difference in approach required to collect this information.

4.3 Risks Relating To The Company Generally / Top Tier Risks

As discussed with PT XYZ'S Chief Operation Officer in Appendix 2, these below risks that are assessed by the company have the potential to materially affect the company's business, results of operations or financial condition.

4.3.1 Legal and Regulatory Issues

a) PT. XYZ is subject to significant exposures arising from "errors and omissions" claims. PT. XYZ provides numerous professional services, including the placement of insurance for corporate and public clients around the world. As a result of these activities, the company is subject to a significant number of errors and omissions, or “E&O”, claims. In our risk and insurance services segment, such claims include allegations of damages arising from failure to adequately place coverage or notify insurers of potential claims on behalf of clients. In our consulting segment, such claims include allegations of damages arising from our consulting services, which frequently involve assumptions and estimates concerning future events. E&O claims seek damages, including punitive and treble damages, in amounts that could, if awarded, be significant and subject us to potential liability for monetary damages, negative publicity, reputational harm and to diversion of personnel and management resources. Given the unpredictability of E&O claims and ligitation, it is possible that an adverse outcome in a particular matter could have a material adverse effect on the company’s businesses, results of operations, financial condition or cash flow in a given period.

b) Without neglecting best effort put in place to comply, the Company’s compliance systems and controls cannot guarantee that it is in compliance with all potentially applicable laws and regulations. This in return, may have an adverse effect on our business.

c) Improper disclosure of personal data could result in legal liability or harm our reputation. The company has certain obligations to maintain the security and privacy of clients’ and employees’ confidential and proprietary information. The company maintain policies, procedures and technological safeguards designed to protect the security and privacy of this information. Nonetheless, the company cannot entirely eliminate the risk of improper access to or disclosure of personal information. Such disclosure could harm reputation and subject the company to liability, resulting in increased costs or loss of revenue or impairment to reputation in marketplace.

4.3.2 Financial Risks

a) Result of operations could be adversely affected by economic and political conditions and the effects of these conditions on clients' business activity. Factors such as local government actions, legislation changes.

b) The inability to successfully recover should the company experience a disaster or other business continuity problem could cause material finacial loss, loss of human capital, regulatory actions, reputational harm or legal liability. Should the company experience a local or regional disaster or other business continuity problem, such as an earthquake, hurricane, terrorist attack, pandemic, security breach, power loss, telecommunications failure or other natural or man-made disaster, it's business continuance will depend, in part, on the availability of personnel, office facilities, and proper functioning of computer, telecommunication and other related systems and operations. In such an event, global operational size, multiple brother companies, and our IT systems (i.e backup) would provide an important advantage.

4.3.3 Competitive Risks

a) The company is operating in a highly competitive environment. If fail to compete effectively, business and operations will suffer. There's a fierce competition in the market. Some competitors do provide free services and offer price cut down to clients, making it difficult for PT. XYZ to retain or attract clients who valued price over other service qualities.

b) The loss of key professionals could hurt the ability to retain existing client revenues and generate revenues from new business. It is therefore very important to retain significant revenue-producing employees and the key managerial and other professionals who support them. The company face numerous challenges in this regard, including :

- the intense competition for talent
- the general mobility of professionals

- the dificulties face in offering compensation of a type and amount (including equity-based compensation) sufficient to attract, motivate and retain valuable employees.

c) Rapid technological changes and failure to adequately anticipate or respond to these changes could adversely affect business and result of operations. To remain competitive, the company indentified the most current technologies and methodologies and integrate them into service offerings. If the company do not make the correct technology choices or investments, or if the choices or investments are insufficiently prompt or cost-effective, business and results of operations could suffer.

4.4 Risks Relating to The Company Specifically / Bottom-up Risk Assessment

Based on documentations provided by the management and as elaborated further during discussion with PT XYZ'S Chief Operation Officer in Appendix 2, these are the company's assessed specific risks cumulated through bottom-up mechanism and it is divided into eight risk categories :

4.4.1 Asset Management / Strategic

4.4.1.1 Denial of Access to the Company's Location

Fire or other incidents occur at neighbor's site which leads to inability to access PT. XYZ's location. This is considering PT. XYZ's office location nears central goverment legislative building which oftenly get ambushed due to demonstration related activities. In return, it might expose PT. XYZ to denial or difficulties to access office premises. The regional Business Resilience Management (BRM) together with local BRM coordinator are constantly in pace and closely monitor, any activities that could lead a halt to business such as major strikes, demonstrations that take place near the office.

4.4.1.2 Theft of assets (i.e computer/data, records, money, staff property, etc)

Breach of security. PT. XYZ imposes “Corporate Security” to encounter the risks that believed leads to company’s lost of assets :

Personnel Risks

In the economic downturn, motives for employee misconduct are on the rise. Increased potential for low morale and high tension surrounding layoffs combined with personal economic pressures on employees create unanticipated personnel risks for companies.

These risks can be mitigated through employee background screening, a universal best practice for corporate security. Given the high proportion of incidents that originate from within organizations – from workplace violence to data theft – it is essential to run checks on potential employees, vendors, and contract personnel. An informed hiring manager is in a better position to make good decisions about whom to trust with the company’s assets and reputation.

Pre-employment background screening needs vary both by industry and by the employee’s position. A credit check is likely unnecessary for an employee who will not be acting in a financial role, but companies will find it valuable to perform criminal record checks on all new employees. Employment and academic verifications can be an important tool for ensuring that an applicant has the appropriate credentials. Résumé fraud may not indicate that the individual is a security threat, but it is a warning sign for possible future misconduct.

Information security risk

History shows that virtually every technological advance can be misused. In the world of digital information, the abusers become the hackers, cyber terrorists, and data thieves reported in the media. Information technology has become an increasingly important front to defend, especially in light of the fact that more than 90% of business information is held in a digital format and approximately 70% of that data is never printed on paper. This information includes everything from sensitive documents and proprietary plans to customer records and employee data. For PT. XYZ, that store personal information about customers or employees, the economic and reputational losses resulting from a data breach can be severe.

Cyber security risk

Most often, information security incidents originate within an organization. To avoid information leakage, PT. XYZ creates and enforces a policy governing the use of their information assets. This include rules relating to employee use of e-mail, websites, media sharing sites, social networking, and instant messaging.

An employee traveling with an encrypted laptop might assume that the corporate data on that computer is secure. The laptop system only invoked absolute protection when the computer was turned off completely. If an employee inserts unknown USB into their computer, it can infect the machine with malware that can be used as the basis for attacking the company’s network and stored data.

Essential cyber security prevention measures is supplemented with detection tools and response plans. On the network level, this involve setting up a Security Operations Center (SOC), installing network sensors that can collect the data needed to identify threats to the network and communicate them to a monitoring center where specialists can look for problems on a 24/7 basis. In crisis situations requiring immediate assessment of cyber-security preparedness, IT colleagues can deploy a “Rapid Deployment Network Sensor Array and Monitoring Package,” otherwise referred to as a “SOC in a Box."

Businesses and other organizations that collect and store personal information such as PT XYZ face special security risks. Organizations are facing the responsibility to protect data, investigate incidents, and take steps to retrieve lost data. In general, the consequences of noncompliance can be severe, potentially resulting in financial penalties, victim or shareholder litigation, loss of customer confidence, and lost sales revenue.

The problem requires a multi-dimensional solution. Both high-tech and low-tech identity theft attacks hinge on corporate vulnerabilities that facilitate the pilfering of sensitive customer data. Attacks can often be thwarted with the right preventative measures. Among them:

- Keeping software current with security updates.
- Knowing where important customer data resides.
- Collecting evidence when an incident occurs.
- Recognizing the risks of wireless data transmission.

In the event of a data breach, it is important to quickly understand what, why, and how it happened. Security problems will likely need to be remediated, and forensic analysis will be necessary to quantify the scope of the breach. Individuals whose personal information has been compromised must be notified, which can be a challenge as legal requirements vary.

Intellectual property risk

Intellectual property (IP) is another intangible asset to be managed and protected. Given the high-value and highly portable nature of IP, it is under increasing threat, especially as companies reduce staff in the wake of market turmoil. Employees who feel aggrieved may decide to leave with the company¡¦s trade secrets, customer lists, pricing, or other sensitive data. IP protection requires attention to both information technology and physical security. It is critical to take proactive IP protection steps:

- Conduct an IP audit.
- Design enforceable IP rights.
- Know the local partners, wherever they are.
- Know your supply and manufacturing chain.

IT security low attention and low budget risk

Corporate security budgets balloon in boom times or, more often, in response to an increase in perception of threat. However, in the wake of the global economic crisis, physical security budgets shrink. Risks continue to evolve, and the tactics of those who seek to do harm will always adapt to changing security postures. All physical security plans require regular audit, testing, and review to ensure that procedures, systems, and training are current and hence budget are one of the important factor for management's attention.

Integrated design and concentric circles of protection risk as a way of a precaution measure in dealing with such IT security issues. Integrated design for site perimeters is already common practice for high security applications and companies now increasingly opt for this more comprehensive approach in new construction. Integrated design combines the architectural features of Crime Prevention Through Environmental Design (CPTED) with traditional technical, physical, and operational security elements. PT XYZ is of the opinion that effective application of CPTED concepts results in architectural features that are barely recognizable as perimeter defense, but instead are presented as well-planned architectural designs. Perimeter security often takes a layered approach, establishing a set of concentric circles. With this layered approach, PT XYZ can control access to their environment further out, ensure that undesirables have several hurdles to breach before reaching critical areas, and gain crucial time to respond to the threat.

4.4.2 Business Model / Change Management

- PT. XYZ has no distinguishing features and consumers buy solely on price. Lack of competitor analysis / corporate intelligence. This is as result of competition pressure and nature of clients who are mostly price conscious. The competition and price overrides a proper strategy. There's a tendency to value price more then other services. The management is actively looking for ways to improve their current position in the market emphasizing global market specialization and knowledge it brings, especially for areas that not all competitors can compete on such as insurance in marine, aviation, energy and infrastructure.

- Lack of close collaboration with other departments, e.g. cross selling. No incentive and no communication related to cross selling. Recent months ago, PT. XYZ starts activating a cross-selling incentive program. In which for any successful referrals will be bonus awarded both for individuals and departments. This applies to all department and individuals, including those from support team. The result of this collaboration is still unavailable when this thesis was made.
- Difficult to penetrate into local businesses and thus halt the business growth speed. There's still lack of awareness in the market to use broker services. PT. XYZ proactively introduce their company and the significance role and benefits that they may bring to clients and potential clients. This is to support the growth of new, renewal and expanded business in the future. Pre-approved special time and budgeted fund was granted to some of team leaders and executives within the company to reach clients and potential clients.
- As result of competitive risks, there's a tendency to do a non-standard pricing models and perceived competitive pressures to discount. Pre-approved invoice by team leaders and monthly revenue review by country leader are prerequisite by PT XYZ to mitigate this risk.

4.4.3 Compliance

Illegal activities by staff, e.g. serious violations of company rules, unauthorized entertainment and / or gift. The risk driver is ethical risk from senior management / decision-makers; business pressure; management control not strict enough. Compliance and Internal audit plays a significant role to check the potential compliance related issue. Their findings will help PT. XYZ to detect any fraud and propose suggestion on how to prevent such illegal activities in the future.

4.4.4 Financial

4.4.4.1 Currency / Foreign Exchange Fluctuations

Country risk; no detailed analysis or effective controls / tools in place. The complex nature of foreign exchange fluctuations makes the analysis becomes difficult. It involves manual estimation (i.e determine hedging to minimize the forex impact) and limited available information. PT. XYZ's most transactions and accounting records is booked under IDR currency but for reporting purpose it used USD currency. This create foreign exchange implications and exposure for the company especially in the case of foreign exchange loss.

4.4.4.2 Unacceptable Levels of Bad Debt Write Off

In a business, bad debt write off is sometimes unavoidable in circumstance where the client is going out of business, or neglect their obligations to pay. Thus making it uncollectible. Currently, the company performed a more thorough risk assessment than before to assess creditworthiness of clients. Collection dept also utilized to perform the job.

4.4.4.3 Failure to Manage Cash Flow / Liquidity

Irregular observation; inappropriate analysis; methodology. Excess cash are now under close supervision from regional finance and accounting team. A regular excess cash report must be submitted to the regional with information on how to manage such funds (time deposit, etc).

4.4.5 Information Technology (IT)

- Frequent failure of IT system (software e.g. servers, telecommunication, etc.). The failure of IT system may be contributed by several factors, such as usage of obsolete equipment, pirate software installed by employees, non-standard applications downloaded may contained virus or crash with exising applications, network bandwith limitation, etc).
- Limited network bandwith. Currently IT Dept use bandwith capacity of 1.56 Mb. The utilization rate is reaching a yearly average of 75%. This is a high utilization in comparison with PT. XYZ's sister companies globally. In certain circumstances the network is so highly utilized that makes all PC's, laptops and systems in the office slower

than usual. Making the work less efficient and less accomodative to support company’s plan to expand the business in the future.

4.4.6 People

4.4.6.1 The Injury of Key Personnel

In absence of injured key personnel in a decision required situations and no proper delegation of authority, could bring risk to the company that the business is not well run.

4.4.6.2 Employees at Risk of Disease and Sickness

In general this risk is due to each employees are exposed to any major pandemic/epidemic incidents. In particular this risk is due to the working environment and style. Most of employees frequently are working until late after normal office hour and more than normal 8 working hours/day. This expose employees to overworking situations and health problems.

4.4.6.3 Loss of Senior Management and/or Entire Team

In the past 2 years there’s a high turnover within the company came from all the departments mostly senior and experienced level. Reaching 10-15% rate. Loss of Senior Management and/or entire team resulting in the loss of intelligence capital, client relationship, etc. This indicates lack of employee retention plan; uncompetitive reward system; poor or lack of succession planning. The management has seriously reviewed the benefit package of each employee during the year to ensure it’s competitiveness in the market. This year new benefit package has been announced to match the market.

4.4.7 Products/Services

- Claims or allegation by clients emanating from a PT XYZ employee's faulty performance or negligence causing error and omission. PT. XYZ is currently having the Error & Ommissions (“E&O) insurance coverage placed by its parent globally. This insurance in particular is to protect the company from cost damage resulting from any legal lawsuits, repay client’s damage compensation cost and other related costs.

- Unable to deliver high quality services to clients. Solely rely on third party e.g. insurance company. There’s a tendency for some brokers to overrely to insurance company works because of the perceived quality and past performances. PT XYZ do have a standard mechanism in place to review any papers (i.e insurance policy, quotation slip, placing slip, etc) to ensure its consistency and accurateness. This will help reduce the E&O risk and reputation damage.

4.4.8 External

Indirect damage to the environment. Over usage of paper and printing. Each employee balance scorecard are now incorporating paper and printing cost/usage reduction.

4.5 Business Continuity Management : The Implementation

The implementation of Business Continuity Management is reflected through the business continuity plan. Three phases of the business continuity plan:

4.5.1 Emergency Response Phase

Emergency Response Phase outlines the procedures required to respond immediately to any incident that may jeopardise the safety of employees, disrupt daily operations or bring unwarranted external scrutiny to the firm. It is the firm’s intent to conduct itself with the highest regard for the safety and health of employees and to protect and preserve its property. The purpose of the Emergency Response phase is to provide guidelines to:

- Ensure the safety and health of employees
- Quickly identify and respond to incidents that may arise at or near the office
- Help evacuate the building in an orderly manner, if necessary
- Assess any damage or impact of a situation
- Ascertain the level of containment required to limit damage to facilities and equipment
- Identify and apply the necessary emergency activities

- Coordinate with local emergency services and authorities
- Manage and communicate information about the incident to the regional BRM Group, Crisis Management Team (CMT) and any other parties deemed necessary
- Notify Global Business Resilient Manager (BRM) Management via the company Emergency Hotline

Recovery Action Plan – Phase 1 – Emergency Response

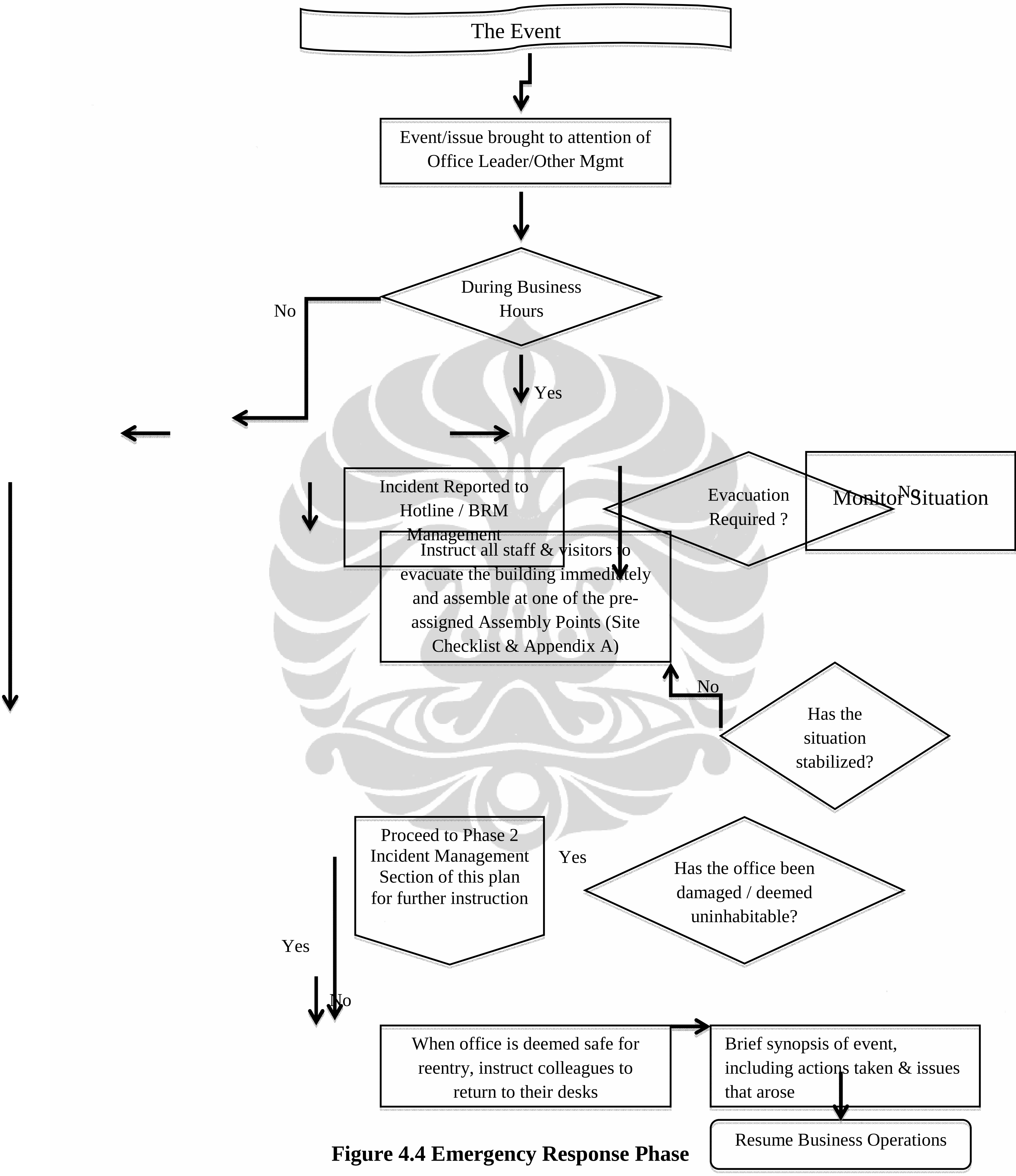
The Event
Event/issue brought to attention of Office Leader/Other Mgmt
During Business Hours
No
Yes
Incident Reported to Hotline / BRM Management
Evacuation Required ?
No
Monitor Situation
Instruct all staff & visitors to evacuate the building immediately and assemble at one of the pre-assigned Assembly Points (Site Checklist & Appendix A)
No
Has the situation stabilized?
Proceed to Phase 2 Incident Management Section of this plan for further instruction
Yes
Has the office been damaged / deemed uninhabitable?
Yes
No
When office is deemed safe for reentry, instruct colleagues to return to their desks
Brief synopsis of event, including actions taken & issues that arose
Resume Business Operations

Figure 4.4 Emergency Response Phase

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

4.5.2 Incident Management Phase

The Incident Management phase addresses the decision processes that follow the onset of an extended outage or disaster. This phase assumes that the local BRM Group will liaise with the regional BRM teams to provide assistance with such areas as: Communications, Technology, Legal, Facilities, Human Resources, and Finance.

The purpose of the Incident Management phase is to ensure:

- Steps necessary to safeguard the welfare of the employees are taken
- Determination of the extent of the incident is accurate
- Appropriate individuals are assembled into response teams to carry out the required actions
- Effective communication is made to employees
- External communications are properly controlled
- Appropriate operating strategies are implemented

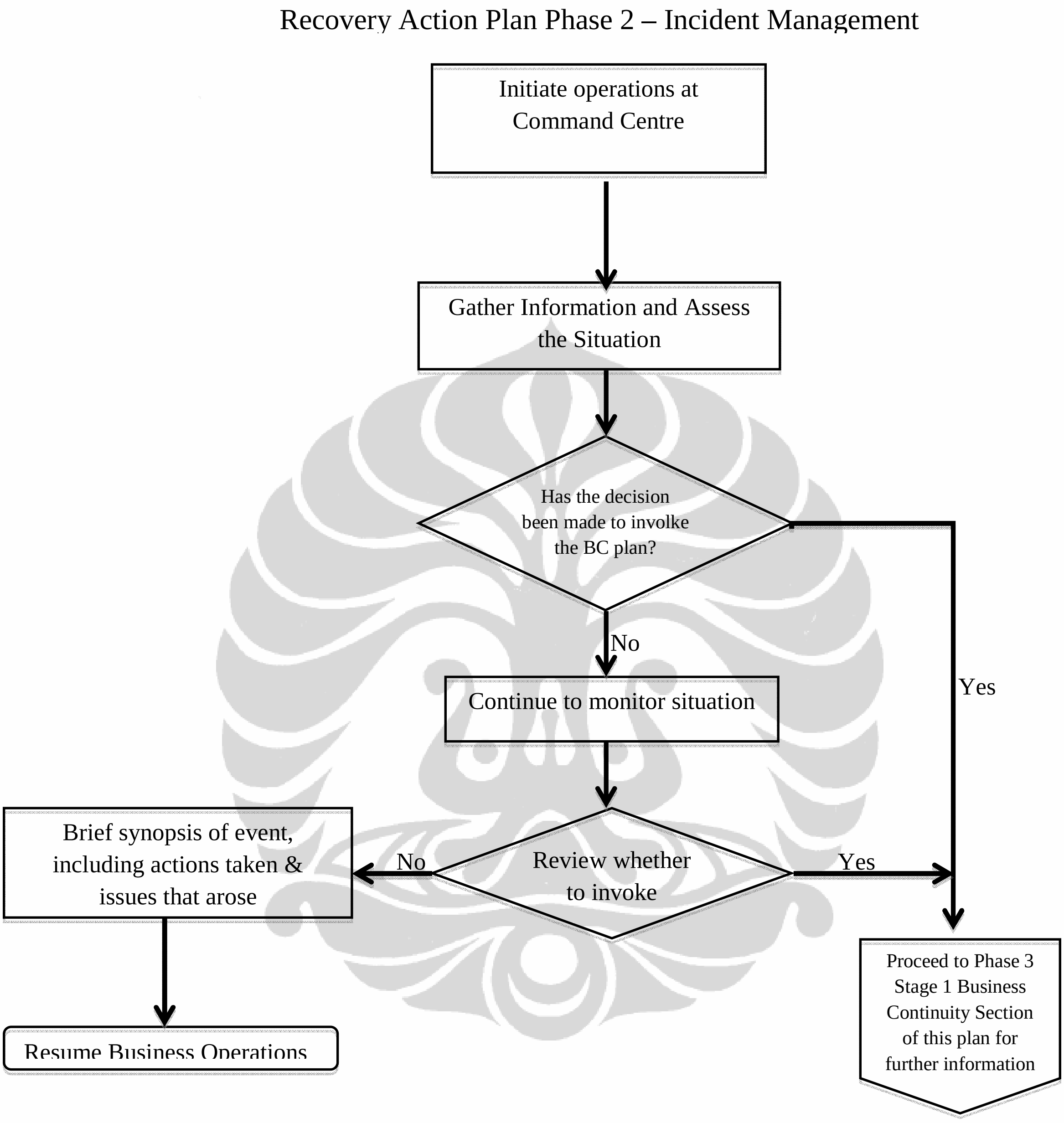
Recovery Action Plan Phase 2 – Incident Management
Initiate operations at Command Centre
Gather Information and Assess the Situation
Has the decision been made to involke the BC plan?
No
Yes
Continue to monitor situation
Review whether to invoke
No
Yes
Brief synopsis of event, including actions taken & issues that arose
Resume Business Operations
Proceed to Phase 3 Stage 1 Business Continuity Section of this plan for further information

Figure 4.5 Incident Management Phase

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

4.5.3 Business Continuity Phase

Business Continuity Phase is designed to provide each line of business with a framework on which to resume critical business processes if an incident disrupts their normal work location and the resources in it are not accessible. The purpose of this phase is to ensure that necessary business conducted at this location can be recovered within reasonable timeframes and to acceptable levels, to ensure our ability to support our clients in an appropriate manner.

Table 4.4 Business Continuity Phase – stage 1

	Phase 3 – Business Continuity
	Stage 1 – Initial Recovery Activities
( )	At the Command Center, the site BC team will meet to initiate the recovery of the critical business processes
( )	Critical Business Functions agree on critical operations, priorities, staffing requirements and work in hand
( )	Agree which members of staff are to be relocated (taking into consideration family commitments, travel difficulties & business requirements)
( )	The BRM Group will invoke the required recovery service providers below in line with business requirements : ▪ Recovery Solution Providers ▪ Internal Sites ▪ Commercial recovery service providers (only if contract is in place) ▪ Other local site (predefined, such as hotel, conference center, etc.)
( )	If Access to disaster site allowed, ascertain which of your documents / personal / salvageable items are required
( )	Recall records from off-site storage, if necessary
( )	Working with the BRM Group, request telephone redirection processes to commence based on an agreed priority list. Look at providing additional telephone operator/reception assistance at location receiving redirected calls.
( )	Depending on office recovery arrangements & staff numbers, establish required transportation provisions and other logistics requirements.
( )	Initiate departmental Call Tree for critical staff. Reiterate the current status and provide assistance as necessary and possible, defined recovery strategies and schedule for implementation. Be careful to relate to colleaques their specific role, responsibility and location for the recovery process. If colleagues have been designated for “On Call” status, reassure them that they will be brought into the recovery process as soon as possible, according to the recovery resources that are, or will become, available.
( )	Update the Office Status Line with current status, defined recovery strategies, and schedule for implementation
( )	Notify the Post Office to hold mail until instructed to resume services
( )	Consider any special client requirements and agree any time of business specific details for client or supplier communication
( )	Ensure all visitors/clients expected to visit the disaster site are informed of any changes to meeting venues.
( )	Summarize, agree & document actions/owners regulary during meeting

Table 4.4 Business Continuity Phase – stage 1 (Continued)

	Phase 3 – Business Continuity
	Stage 1 – Initial Recovery Activities
( )	Agree next steps & nest team meeting, try to ensure that the team meets as the start & end of the day whilst incident is critical then as necessary thereafter
( )	Update Line of Business Leaders, local BCP Team Leader/Alternate with team status, actions.
( )	Transport appropriate colleagues to their associated recovery sites.
	- Colleagues Arrive At The Recovery Site(s) -

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

Table 4.5 Business Continuity Phase – stage 2

Phase 3 – Business Continuity					
Stage 2 – Restoration of "Business as Necessary"					
Business Related		**Technology Related**			
( )	Arrive at recovery site	( )	Verify contracted resources are available		
( )	Establish mail sorting area and procedures	( )	Initiate additional resources procurement processes		
( )	Contact the Post Office and resume mail delivery to the mail sorting site	( )	Initiate build of PC's using Staff names relocating to recovery site		
( )	Verify any vital records delivered by the off-site storage provider. If there are missing items, contact the provider immediately and make arragements for the delivery of the missing items.		Processing Platforms		Network/Communications
( )	Initiate manual business processes as soon as possible. Assimilate additional processes into the recovery process as technology and applications become available	( )	Provide technical support as necessary	( )	The Global Network Services group will coordinate any required redirection of the network
( )	Phase in additional technical provisioning as it becomes available			( )	On-site technical support will verify that the required Local Area Networking infrastructure is in place, and is usable
( )	Maintain contact with the key clients to ensure that they have the most current methods for communicating with your office			( )	Initiate redirected telephone service and coverage at the recovery site
( )	Assist technology in the validation of restored processing facilities			( )	Initiate redirected FAX service and coverage at the recovery site
( )	Establish whether any work in progress has been lost and how to recreate lost data			( )	Provide technical support as necessary
( )	Enter "orphan" data (data collected via manual processes following the disaster/outage)				

Table 4.5 Business Continuity Phase – stage 2 (continued)

Phase 3 – Business Continuity					
Stage 2 – Restoration of "Business as Necessary"					
Business Related			Technology Related		
( )	Validate the status of the restored/recreated/entered data. If the status of the data/applications is satisfactory, merge the newly available processing environment to production status				

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

Table 4.6 Business Continuity Phase – stage 3

Phase 3 – Business Continuity					
Stage 3 – Ongoing Recovery Processes					
Business related		Processing Platforms		Network / Communications	
( )	Assimilate additional business processes/staff into the recovery flow as they become available/required	( )	Provide technical support as necesarry	( )	Provide technical support as necesarry
( )	As changes in recovery status occur, the BRM Group will keep management and the CM Team updated				
( )	Recovered critical functions now operating from Recovery location				
( )	Monitor and regulary review and back log of work – prior to incident/post incident				

Source : PT XYZ's internal documentation combined with additional information obtained during interview with the Chief Operation Officer. Refer to Appendix 2.

The plan further makes the following *General Assumptions*:

- The recovery site(s) will be used for the minimum resources necessary to resume critical operations in the shortest possible time. It will not be used to restore a full complement to a business-as-usual state.

- Trained personnel familiar with the operations of the office and its lines of business are available for implementing the recovery process and trained personnel from other sister offices will be available to assist them.

4.6 IT Strategy Practices

PT. XYZ establishes internal controls to ensure protection of its information assets, and to comply with business and regulatory requirements. These controls, which include related planning, development and implementation of appropriate policies and procedures, are reviewed regularly and updated where applicable to ensure the integrity, availability and confidentiality of corporate and client information.

The following provides a summary of related practices and controls as provided in internal documentations and during interview with the Chief Operation Officer :

4.6.1 Risk and Security Organization

PT. XYZ has established risk management and information security teams that are responsible for assssing business risk and preparing, reviewing and testing plans to maintain business operations, establishing and implementing security policies, and advising on implementation of security products and procedures that comply with its policies. The firm employees, contractors and vendors are responsible for compliance with all applicable policies and procedures.

4.6.2 Confidentiality

All employees agree to abide by the Company's *Code of Business Conduct & Ethics.* This document covers various aspects of working at the firm and for our clients. The Code of Business Conduct & Ethics includes a section specifically addressing confidentiality of client data and information and an employee's obligations therein.

4.6.3 Business Resiliency and Disaster Recovery

A cornerstone of PT. XYZ's client relationships is the commitment to the integrity and security of client information and to our continuation of services, even in the event of a disaster. To support that commitment, PT. XYZ strictly adhere to business resiliency/disaster recovery plans that cover our ability to serve our clients during a disaster scenario.

Based on interview with IT Dept Head as quoted from Appendix 2 of this thesis, the program includes mandates maintainance of business resiliency / disaster recovery plans with specific provisions for staff mobilization, alternate work spaces

Plans are tested annually and updated as necessary to address deficiencies or identified gaps.

4.6.4 IT and Information Security

Access Controls and Information Handling

- Users are required to use a unique ID to access application and network resources.
- Accounts are removed immediately following employment termination and/or when access is no longer needed. Where applicable and/or required by regulatory compliance, accounts are reviewed for status and permissions levels. Account changes are performed by authorized personnel using appropriate systems and processes.
- Password controls include defined minimum length, are not displayed on screens or reports, and a history is maintained to prevent the re-use of recent passwords. Accounts are locked after multiple authentication failures.
- Vendor supplied default passwords are required to be changed before a new system can be implemented into production.
- Remote access is restricted to authorized users and secured through virtual private network (VPN) using two-factor authentication with one-time passwords.
- Depending on the sensitivity of data, and associated storage and transmission methods, uses SSL, secure file transfer (SFTP), digital certificates (S/Mime), PGP, and other encryption solutions (e.g., TLS).
- All company laptops and workstations are required to have whole disk encryption installed and enabled.

- Electronic media, such as system hard drives, is required to be sanitized (i.e., digitally overwritten with random characters) prior to re-use or removal from production.
- Hardcopy media containing sensitive information is required to be discarded in locked containers for later shredding/destruction by contracted service providers.

Data Center Physical Security

- Building access is controlled via electronic access control systems (e.g., keycard or bio-metric device) and/or appropriate sign-in (e.g., all visitors must sign in). Access to data center areas is restricted to only those personnel whose job duties require access to such areas.
- Access to data centers is logged for investigative and audit purposes.
- Camera surveillance of data center areas is provided in critical locations and monitored 24x7.
- Operations and data center areas are protected against environmental hazards using dedicated fire response, environmental protection and cooling systems, as well as backup and uninterruptible power supply systems.
- Visitors, contractors and vendors are not permitted into secured areas unless they have operational responsibility which requires such access, the access is approved by Operations management, and the visitor is escorted by authorized staff.
- Operations and Network Management
- All systems and configuration changes must be logged, reviewed, approved and monitored.
- Intrusion Detection Systems and other traffic and event correlation procedures are implemented, maintained and monitored 24x7.
- At the network layer, enterprise firewalls, VLANs, and layered DMZ architectures are used to help protect systems from intrusion and limit the scope of any successful attack.

Vulnerability Management and Incident Response

- A multi-tiered anti-virus and anti-spyware program is in place for e-mail and network gateways, servers, and desktops. Anti-virus signatures are updated daily.
- Security vulnerabilities and alerts are tracked by information security personnel and assessed by appropriate technical experts. Vulnerabilities are ranked in accordance with an internal assessment process taking into account any mitigating factors (e.g., AV coverage, firewall protection).
- The implementation of patches and/or other workarounds are tracked and monitored via Change Management processes
- A global problem/incident management team and processes are in place. The processes are based around ITIL standards and include escalation and notifications procedures. Escalation and external party notification is dependant upon the nature of the incident.

Compliance and Audit

- PT. XYZ complies with the laws and regulations of the countries in which it operates.
- Any transfer of data necessary to fulfill the services we undertake for our clients will be protected by appropriate contractual arrangements in accordance with applicable local, national or regional privacy regulations.
- Audits are performed to verify and maintain compliance with business and regulatory requirements. Audit results are presented in internal findings reports with remediation efforts concentrated on refining or establishing processes and procedures, or implementing technology solutions to fill identified gaps.

4.7 Disaster Recovery Plan Analysis

Disaster recovery plan analysis will use two framework theories as below :

4.7.1 Disaster Recovery Plan Assessment

Disaster Recovery Plan Assessment of PT. XYZ’s using 3-time-phase framework (Reddick, 2011; Choi, 2009; Foster and Dye, 2005; Ritchie, 2004) :

Pre-event Stage

Based on theoretical framework referred from chapter 2, point 2.4.2, pre-event stage should begin with risk assessment of existing condition, including controls in place to mitigate the risks. These are usually steps taken before disaster strikes as precaution in case of emergencies and to reduce the damaged caused by it.

Based on actual practice in PT XYZ that assessed by author through PT XYZ internal documentation and interview results in Appendix 1 & 2, their pre-event stage begins with IT risk assessment. Refer to point 4.4.5 and 4.4.1.2 in chapter 4:

- Frequent failure of IT system (software e.g. servers, telecommunication, etc.). The failure of IT system may be contributed by several factors, such as usage of obsolete equipment, pirate software installed by employees, non-standard applications downloaded may contained virus or crash with exising applications, etc). Mitigating control in place is to revitalize or replace obsolete equipment within it’s usage life before it crashed and resulting in important data loss. Regular maintenance of company’s local server, PC’s and notebooks to ensure no misusage by employees such as installation of non-standard application and virus contained.
- Limited network bandwith. Currently IT Dept use bandwith capacity of 1.56 Mb. The utilization rate is reaching a yearly average of 75%. This is a high utilization in comparison with PT. XYZ’s sister companies globally. In certain circumstances the network is so highly utilized that makes all PC’s, laptops and systems in the office slower than usual. Making the work less efficient. This will halt company’s plan to expand the business in the future. No definite plan yet in place to overcome network bandwith limitation based on data observation and interview in Appendix 2.

- Information & cyber security risk. Information technology has become an increasingly important front to defend. This information includes everything from internal strategy documents, customer records and employee data. The inability to secure these informations could have a severe impact for the company in terms of lost of trust/confidence by its employees and customers, lost sales and potential sales. Not to mentioned litigation exposure if data breach cause a serious loss for the client. The mitigating control is PT XYZ enforcing rules governing the use of their information/assets. This include rules relating to employee use of e-mail, websites, media sharing sites, social networking, and instant messaging. Essential cyber security prevention measures is supplemented with detection tools and response plans. On the network level, this involve setting up a Security Operations Center (SOC), installing network sensors that can collect the data needed to identify threats to the network and communicate them to a monitoring center where specialists can look for problems on a 24/7 basis. In crisis situations requiring immediate assessment of cyber-security preparedness, IT colleagues can deploy a “Rapid Deployment Network Sensor Array and Monitoring Package,” otherwise referred to as a “SOC in a Box." In addition, the IT global team have an integrated design combines the architectural features of Crime Prevention Through Environmental Design (CPTED) with traditional technical, physical, and operational security elements. The most effective application of CPTED concepts results in architectural features that are barely recognizable as perimeter defense, but instead are presented as well-planned architectural designs. Perimeter security often takes a layered approach, establishing a set of concentric circles. With this layered approach, organizations can control access to their environment, ensure that undesirables have several hurdles to breach before reaching critical areas, and gain crucial time to respond to the threat.
- IT low attention and low budget risk. IT budgets balloon in boom times mostly in response to an increase in perception of threat. However, in the wake of the global economic crisis, we have seen IT budgets shrink. Despite

the fact that risks continue to evolve, and the tactics of those who seek to do harm will always adapt to changing security postures. The mitigating control is that security plans are must have a regular audit, testing, and review to ensure that procedures, systems, and training are current and effective. Should there any indication of IT malfunction or ineffective, it needs to be addressed as soon as possible and budget are allocated accordingly.

The analysis is that in actual condition as explained above, PT XYZ did assess their risks especially IT risks. They recognised the risk of inherent IT system failure, Information and cyber security risk whereas data breach could bring a disaster to the company, IT low attention and low budget from management and limited network bandwith. Each risks are equipped with it's corresponding risk mitigating activities to enhance the readiness of organizations in respond to business interruptions including disasters. However, the latter point (limited network bandwith) has no risk mitigating controls in place. The impact of having no respond over limited/highly utilized bandwith could contribute to slower network and system making the work less efficient due to time spent on system. There is a need for PT XYZ to upgrade their current bandwith to support current data flow and PT XYZ's growth. This is point of recommendation included in chapter 5.

During the Disaster

Based on theoretical framework referred from chapter 2, point 2.4.2, this stage requires implementation of strategies to deal with its impacts. In DRP-IT context, these are the information technology activities undertaken immediately following a disaster to provide emergency assistance to those in need and minimize property damage, such as emergency plan activation, activation of emergency systems, emergency medical assistance, shelter and evacuation, and research and rescue.

Based on actual practice in PT XYZ that assessed by author through PT XYZ internal documentation and interview results in Appendix 1 & 2 is that during disaster, the BRM leader (the country leader or CEO) will activate the BCP including DRP as part of it, as deemed critical to do so, by coordination and consultation with Regional Business Resilience Team. The company's detailed business continuity plan comprised of emergency response phase, incident management phase and recovery phase as described in Figure 4.4, 4.5, Table 4.4, 4.5 and 4.6 in chapter 4. In such plan, technology role is clearly formulated starting from immediate report to regional asia pacific Business Resilience Management (BRM) team about the damages related to IT infrastructure; start containing to limit the damage; coordination with local and overseas vendor to retrieve data, supplies and required IT equipment (i.e servers, notebooks, etc); prepare the recovery site as deemed needed if the office premises is no longer usable; looking for assistance to repair LAN network infrastructure in place that is damaged due to disaster; initiate redirection telephone and fax services to be diverted to recovery site or temporarily disactivate until further notice. These are the minimum actions that need to be done by the IT team but there is no rigid sequence. The priorities will then need to be assessed on disaster by disaster basis. During disaster, the command centre is the centre for command, control, information and liaison between various parties including employees, media, etc. IT team will also look to this command centre for direction, assistance, information, and reporting. For PT. XYZ, the command centre is located in one of employee's nearest house from the office.

The analysis is that PT XYZ covers their disaster containing activities through activities performed in sequence basis. First emergency response phase (Figure 4.4) followed by incident management phase (Figure 4.5) and recovery phase (Table 4.4 and 4.5). Not all being followed, it will decided based on discretion of country leader / CEO and COO in coordination and consultation with regional Business Resilience Team (the team who is responsible on the implementation of BCP). Some of recovery phase performed during Post-event stage. As mentioned in point 4.5.2, PT XYZ will activate the incident management phase to safeguard the wellfare of its people and make an effective communication to employees.

Other examples are to initiate departmental Call Tree for critical staff. Reiterate their current status and provide assistance as necessary and possible. This spirit is inline with the theory which mention about providing emergency assistance to those in need. As to minimize property damage, in business continuity phase in Table 4.4, if access to disaster site is allowed, ascertain documents / personal / salvageable items to be collected as required. This is part of PT XYZ's effort to retrieve its valuable data and minimize property damage. From DRP – IT point of view, the effort during disaster comprise of report to regional Business Resilience Management (BRM) team about the disasters related to IT infrastructure; coordination with local and overseas vendor to retrieve IT related data and equipment; prepare the recovery site as deemed needed if the office premises is no longer usable; looking for assistance to repair LAN network infrastructure in place that is damaged due to disaster; initiate redirection telephone and fax services to be diverted to recovery site or temporarily disactivate until further notice. These are all activities reflecting efforts put to contain the disaster, minimize its impact and put best effort to get back into business soon.

Post-event Stage

Based on theoretical framework, Post event stage is the phase in which a long-term recovery or resolution phase allowing for evaluation and feedback into future prevention and planning strategies. Also to recover at least to the pre-disaster condition of well being.

Based on actual practice in PT XYZ, post event phase comprises of several stages that are Initial Recovery Activities, Restoration of Business as Necessary and Ongoing Business Recovery Process. This is fully described in Table 4.4 – 4.6. Also, after an event take place and situation has stabilized, PT XYZ must create brief synopsis of such event, including actions taken & issues that arose. Regular monitor and review and back log of work prior and post incidents are also being documented.

The analysis is that PT XYZ's practice covers activities with aim to achieve long term recovery, stronger IT infrastructure through evaluation and fedback. During IT recovery phase, one of notable process is that once the system are recovered and now able to support normal business operation, the next process is to take lessons learnt from such disaster. A report need to be prepared as soon as the situation back to stable state. This report is used for internal and regional/global purpose as their reference to better deal with disaster in the future. This report is usually will be incorporated into the firm's next periodic risk management analysis/assessment. This is a good practice to prevent the recurrence of same disasters in the future if ways to prevent it can be learnt and implemented.

4.7.2 Recommended IT Recovery Strategy

Recommended IT Recovery Strategy including consideration aspects such as infrastructure, applications, and data management as suggested by Wallace and Webber (2011) :

4.7.2.1 Recovery options for workplace

Wallace and Webber (2011) emphasize the importance of having work area recovery plan in place that is preparing workspace to temporarily support recovery of business operations. Out of several options as described in chapter 2 (2.3.3), PT. XYZ choose recovery strategy of contracted hot site. If the disaster effect only takes 2-5 days, then the firm is opt to use hotel conference rooms as the temporary workplace but if it is more than 1 week time, the company has it's preferred vendor locates in different district with the office ("preferred recovery site"). The vendor provides all the basic requirement of an emergency workspace such as table, chair, PC's, access to network, separate telephone line/different telephone operator and some space for server. The analysis is that this would be a good option for PT XYZ as it can recovers from disaster quite fast in comparison to other options such as rental empty space (estimated activated time around 24 hours). The preferred vendor site already equipped with the required security, telecom and bandwith capacity and the location is relatively near (employees could reach within approximately 1 hours driving range from Jakarta).

4.7.2.2 IT Recovery Strategy

IT Recovery Strategy as suggested by Wallace & Webber (2011) includes rebuilding :

- Enviromental

  Based on theoretical framework, IT equipment must stay within a specific temperature and humidity range. Actual preference by PT XYZ is using a contracted hot site. The analysis is that if use a hotel as a temporary base then there is a limitation on the network capacity and speed of working connectivity. The environment only able to support comfortably in a short period of time. If extended, the cost might be high and there's a capacity limitation. In constrast with hotel, based on facility tour to the preferred vendor, the preferred recovery site has the required temperature and humidity for servers. The workspace also condusive as a temporary working site for critical business functions until the office up and running again. This vendor besides of providing such site also provide the related accomodations (restaurants and lodge for employees should needed). PT XYZ's opt are in favor in terms of security, telecommunication and bandwith capacity, and time to activate. The highly relatively cost is worthed if the company is able to up and running, faster and more efficient in comparison to competitors, thus create value added for clients. Client who perceived values might pay premium prices.

- Infrastructure

  Based on theoretical framework in chapter 2, point 2.4.3, external network must provide connection into the data centre of the local service provider and throughout the recovered data centre. The actual condition is that PT. XYZ's local area network (LAN) is part of the bigger network or wide area network (WAN) connecting sister and parent companies globally. PT. XYZ locally maintain servers in a server room and by using LAN connecting the servers to all the printers and computers. The network is using the client/server type of relationship, means each end user PC's or printers are connected to a central server, which coordinates communication and supplies resources to the end users. The servers contains file storage, printer, backup tape drive and other resources that are shared by the end-user client computers. The network connection of PT. XYZ are basically maintained by global IT team in which they monitor the system on 24/7 basis for any anomalies (i.e virus attack, etc). The analysis is that there's a minimum responsibility for local IT team as almost all aspect of IT are in the hand of regional IT team. Local IT team are in responsible only for local server, local data maintenance, monitor current infrastructure, report any anomalies and support regional activities / project. In case of disaster, their regional IT team will be of the assistance to provide the required application, equipment and technical assistance. PT XYZ through IT Dept Head already make sure, based on interview in Appendix 2 that their preferred vendor able to provide the required infrastructure to enable PT XYZ to connect their data centre throughout to recovered data centre.

- Applications

Based on theoretical framework, Company specific software used by the business to address customer and internal administrative requirements. The detailed applications :

- Prerequisite systems/applications that are required prior to restoring this application
- Successor systems/applications that are fed by this application
- Application or infrastructure component license requirements

In practice, PT. XYZ uses a various business applications namely such as eGlobal, iMAP, iExpenses, and Oracle. IT Team has a special disk containing a standard image of every notebook or PC's in the company. The disk is kept in the office and the copy is kept by the IT Dept Head's home. By keeping such imaging disk, in case of no notebook or PC's are working using the standard configuration, it could help formatting either the existing PC's or notebook or PC's or notebooks located in the recovery site. Should the image disk gone, the IT local recovery team can reacquired it from Regional Asia Pacific IT team who got copies of it. The image data is periodically updated following any changes, if any. The analysis is that there are controls in place for applications to ensure its ongoing usage (that is by keeping imaging disk in office and one copy kept by regional team for easy retrieval in case disaster).

- Data

  The theoretical framework is that the informations are needed by the company's business departments to support the flow of products and services . Hence precaution measures on data need to be done. The actual practice is that there are two types of data that being secured by the company :

  a. Applications data

  b. Data in shared drive

  The analysis are :

  a. Applications data

     Applications data are the responsible of global IT team. They responsible to maintain the data. So data being inputted to Oracle, eGlobal, and other applications will always can be retrieved as long as the asia pacific server is working. The asia pacific server has it's own disaster recovery plan in place to secure all these data.

  b. Data in shared drive

     Datas of employees in the shared drive are daily backed up over night by the local IT team and saved in a specific media storage. This media is picked up every working day by a vendor that will kept it securely tein an off-site storage. It can be retrieved when needed by mentioning the tape number. The IT team also kept copy of backup within office in case needed.

The key to a prompt IT recovery is ready access to the most recent copy of the company's back up media. Every company has its own approach to storing this media. In PT. XYZ , the company is backing-up the data on a daily basis over a night. First thing in the morning, the usual vendor will pick up the data for their storage. The back up media is kept in a location of approximately about 2 hours drive. PT. XYZ paid the vendor a fixed fee in return to data media pickup service, storing the media in it's secured storage, and provide delivery service in case we need to retrieve the media urgently (it able to deliver the back up data less than 1 day for urgent cases).

- Based on Wallace & Webber (2011), there are risks to be considered when assessing data loss. They are viruses, natural disasters, human-created outages, hard drive crash, laptop or smartphone loss or theft, software failures, application failures, vendor failure

The analysis based on company's actual practice:

1. Viruses

   Anti viruses programs are provided and maintained by global IT team. A multi-tiered anti-virus and anti-spyware program is in place for e-mail and network gateways, servers, and desktops. Anti-virus signatures are updated daily.

2. Natural disasters

   The company outsourced its media backup to a third party who store the file in different district with the company's office. The location is about 2 hours drive. In case disaster strikes, the company will still be able to retrieve their valuable data from vendor.

3. Human-created outages

   Systems can be damaged by a sudden power loss. The building host of PT. XYZ's office are reliable in terms of power loss. They have a separate inside building generator as a back up if the normal power is in loss condition. And the generator supplies could last for 3 days operation. Thus it makes the possibility of data loss due power loss is rather small.

4. Hard drive crash

   Since all datas are being backed up over night. The highest risk of data loss is only between last night up to the crash time. It will be rather difficult to retrieve the data. in such circumstances.

5. Laptop or smartphone Loss or Theft

   Attacks can often be thwarted with the right preventative measures. Among them:

   - Keeping software current with security updates.
   - Knowing where important customer data resides.
   - Collecting evidence when an incident occurs.
   - Recognizing the risks of wireless data transmission.

   Any data loss from the night before can still be retrieved.

6. Software Failures

   The regional Asia Pacific IT team are in close supervision of software performance. Any detected potential or issues related to specific software, is raised to the vendor for them to check.

7. Application &Vendor Failures

   Regional IT team who makes arrangement with the vendor makes a clear agreements in which any failure to deliver their service will subject to penalties. This is out of scope of the local IT team who relies on the regional IT team as per designed IT governance.

The analysis is that on each items above to consider as suggested by Wallace & Webber, PT XYZ has take their precaution measures as to mitigate or plan on how to respond to each risk. Based on the above we assess that PT XYZ has taken the needed steps to protect itself from disaster IT threat.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

PT. XYZ's business risks identified through the company's risk assessment procedures categorized into Top Tier Risks (these are risks identified by top level management) and Bottom-Up Risks (these are risks cumulated from bottom-up risk assessment mechanism, that is day to day personnel up to supervisor, manager and then to top management).

1. Top Tier Risks
   a) Error & Omission risks.
   b) Compliance risks.
   c) Breach of data security or confidentiality.
   d) Economic risks.
   e) Business continuance risks.
   f) Competition risks.
   g) Key personnel loss risks.
   h) Technological risks.
2. Bottom-up Risk
   a) Access to the Company's Location risks.
   b) Loss of assets risks. (i.e computer/data, records, money, staff property, etc).
   c) Weak business model risks.
   d) Minimum internal coordination risks.
   e. Business penetration difficulties risks.
   f) Competition risks.
   g) Compliance.
   h) Currency / Foreign Exchange Fluctuations risks.
   i) Bad debt risks.
   j) Failure to Manage Cash Flow / Liquidity risks.
   k) IT failure risks.
   l) Limited capacity risks.

m) The Injury of Key Personnel risks.

n) Employees at Risk of Disease and Sickness.

o) Loss of Senior Management and/or Entire Team.

p) Error and Ommissions risks.

q) Product quality risks.

r) Indirect damage to the environment.

To assess PT XYZ current disaster recovery plan, the analysis uses a combination framework provided by Reddick, 2011; Choi, 2009; Foster and Dye, 2005; Ritchie, 2004 in which the analysis was seggregated into three time based stages, that are pre-event, during and post-event stages. The subsequent framework used is taken from Wallace and Webber (2011), in which it sets out the components of recommended IT Recovery Strategy. We used components proposed such as enviromental, infrastructure, applications, and data as basis to analysis PT XYZ current disaster recovery plan.

Based on such framework based analysis, it is concluded that, PT. XYZ's disaster recovery plan has incorporates step by step actions deemed required based on the underlying theory, to face disasters given the existing IT risks. Some points for improvement are created under the recommendations section below as propositions to better improve their recovery plan in the future.

This thesis has academic implication as it contributes as a future basis of reference for any researchers who interested in studying disaster recovery plan particularly if assessing it by using the abovementioned theoretical framework based analysis. This case study also provides a picture of actual DRP practice in a company, in which if combined with other companies who also using DRP could be used to analyze the DRP contribution to companies in general and also can be used as a cross-reference of best practice DRP to get the maximum benefit of DRP.

This thesis provides managerial implication as it provides direct practical recommendation in below section for PT XYZ to improve their existing disaster recovery plan.

5.2 Recommendations

1. One of the key characteristic of a purposeful business continuity plan ("BCP") is that it is updated regularly whenever applicable changes happen. In PT. XYZ, based on observation and interview, the Business Continuity Plan is not being updated regularly following changes in the organization. The main changes taking place in PT XYZ within the last 2 years were employee changes due to employee turnover. Despite the fact that almost 25% of PT XYZ's employees are new employees joining in the last 1 year, such changes are not periodically updated in the Business Continuity Plan. The last updated Business Continuity Plan is dated back at 4th May 2010. No updated BCP prepared and distributed to department head until now. Management (based on interview with local Chief Operating Officer) is of the position that they're still preparing the BCP before it is ready for distribution but no definite distribution date is known. This creates a risk for the company that some of employees are not well covered within the company business continuity plan during this period of time and when a business interruption takes place, the company will have difficulties to contact or quickly respond to a disaster and informing their employees. Team leaders who doesn't keep detailed information about their employees might lost communication with their team in a disaster event and perhaps need to rely for HR assistance since they kept all the employee personal/contact data. The function of disaster recovery plan ("DRP") as part of the overall business continuity plan, will also be impacted by this condition. A recovered IT function through DRP will be less of usage/benefits if the people intended to utilize it are not available. The recommendation is to put some attention on administrative aspect of the Business Continuity Plan, that is to regularly update the employee lists in the BCP plan at a regular reasonable interval time period, as it will impact the Disaster Recovery

Plan as well if there’s no proper documentation of employees who will then utilized the recovered system. Ideally whenever changes take place, the BCP must be updated instantly to reflect such change.

2. Unadressed risk could evolve into a business interruption or even worse to disaster. One of the recognise IT risk is related to PT. XYZ’s network bandwith capacity. Currently the yearly average usage is 75%, one of the highest in comparison to sister companies globally. Currently the used bandwith capacity is 1.56 Mbps. In certain circumstances/period of time the network usage is so highly utilized that makes all PC’s, laptops and systems in the office slower than usual. Making the work less efficient. As the company planned to expand the business and to recruit new joiners, network bandwith capacity need to be taken into account. Client service aspect also need to be considered as services may come into halt. Stuck system due to overworked network may significantly interrupt business operations. The recommendation is for the company to upgrade their current network bandwith (1.56 Mbps) to at least 2.0 Mbps to accomodate company’s strategic plan. 2.0 Mbps network bandwith capacity is considered suffice and reasonable to support current data flow and at the same time able to support addition of network capacity needed given new recruits in near future (as the company planned to expand and grow it’s business).

REFERENCES

Association of Contingency Planners.. (n.d). *BCP 101*. June 6, 2011. http://www.acp-international.com/know_bcp101.asp.

Begley, S., & Murr, A. (2011). How to save California. *Newsweek* , March 28, 30.

Bill, E. (2011). The impact of disaster. *Newsweek* , March 28, 22.

British Standard Institute. (n.d.). *10 things you should know about business continuity management.* May 31, 2011. http://www.talkingbusinesscontinuity.com/10-things-you-should-know-about-business-continuity-management.aspx

Business Continuity Institute. (2011). Business Impact Analysis, Crisis Management, Disaster Recovery, Disruption, Resilience. In Dictionary of Business Continuity Management Terms (p. 9, 15, 16, 21, 30).

Choi, S.A. (2009). Emergency management: Implications from a strategic management perspective. *Journal of Homeland Security and Emergency Management,* 1, 5, 8, 16.

David, F. R. (2001). *Strategic management concepts and cases* (8th ed.). New Jersey. Prentice-Hall, Inc.

Descriptive research. (n.d). June 7, 2011. http://linguistics.byu.edu/faculty/henrichsenl/ResearchMethods/RM_2_05.html

Foster, S.P., & Dye, K. (2005). Building continuity into strategy. *Journal of Corporate Real Estate*, 105-119. June 6, 2011.

Miller, R. (2011). *Closing the divide between business continuity management and IT disaster recovery*. June 6, 2011. http://www.continuitycentral.com/feature0871.html.

Patton, M.Q. (1990). Qualitative evaluation and research methods (2nd ed.). California: Wiley company.

Pickett, K. S. (2006). *Enterprise Risk Management : A manager's journey.* Canada: John Wiley & Sons, Inc.

Power, M. (2009). The risk management of nothing. *Journal of Accounting, Organizations and Society*, Vol. No. 34, 849.

PT XYZ Intranet

Qualitative Descriptive Research. (n.d). June 7, 2011. http://ahatter.wordpress.com/research-methods/qualitative-descriptive-research/

Reddick, C. (2011). *Information technology and emergency management: Preparedness and planning in US states*, Disasters. 35,7. 45-61.

Ritchie, B.W. (2004). *Chaos, crises and disasters: A strategic approach to crisis management in the tourism industry*, 670, 672.

Rosen, R. E. (2003). Risk management and corporate governance: The case of Enron. *Connecticut Law Review*, 1160, 1165-1167, 1171, 1179. December 11, 2003. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=468168

Starr, R., Newfrock, J., & Delurey, M. (n.d). Enterprise resilience: Managing risk in the Networked Economy. Strategy + Business No. 30, 3-7.

Thompson, D.D. (2010, May). Building effectiveness in multi-state disaster management systems: The case of the carribean disaster and emergency response agency, 2-3. May 2010. ABI/INFORM Global (Proquest) database.

Tinsley, C.H., Dillon, R.L., & Madsen, P.M. (2011). How to avoid catastrophe. *Harvard Business Review*, April, 90-97.

Wallace, M., & Webber, L. (2011). *The Disaster Recovery Handbook* (2nd ed.). New York: Amacom.

APPENDIX 1

EXPLORATORY RESEARCH

Exploratory research : Interview with Chief Operation Officer on 3 June 2011 to gain deeper understanding of existing disaster recovery plan of PT XYZ

Respondent : Chief Operation Officer PT XYZ

Author : “Good morning Bu. As discussed during our meeting previously regarding today’s interview agenda. I would like to elaborate further related to PT XYZ’s existing disaster recovery plan.”

Respondent : “Sure, shoot the questions.”

Author : “It is my believe, before we talk further about disaster recovery plan, that the underlying framework for any disaster recovery plan is a company’s attitude towards risk and how they respond to it.”

Respondent : “Correct. PT XYZ has a risk management policy in place to accomomodate risk. Here i show you the risk management policy being applied. Please make this data anonymous. Do not mention the company’s name.”

Author : “Agree. Will keep it as confidential.”

Respondent : “You can see in the file that i gave you, our Risk Management Policy is quite comprehensive, starting from basic risk definition, company’s risk categorization, objectives and who should suppose to take responsibilities on risk management, overview of risk management framework, risk governance, and risk appetite. But perhaps, i think the important one is related to risk processes. It’s about how we determine our risks. As you can see, we have top-down and bottom-up way of risks assessment. The combination of both are becoming our risk register. Oh. this document might interest you. PT XYZ uses three lines of defense against risk. The first line is our support team, the second line is our compliance and legal officer and the last one is the regional internal audit. With these 3 layers, we do hope we can minimize the risk of doing business.”

Author : “I see. That’s the way you assess and mitigate the risks at the same time. But can i get the actual risk register of the company ?”

Respondent : “Yes you can. But again this is confidential and please put it as anonymous.”

Author : “I will. Thank you. Is it regularly updated ? I mean the risk register?”

Respondent : “Yes, we updated it regularly. The one that i gave you is the latest one around end of last year or beginning of this year.”

Author : “What is the connection between risk policy, risk governance, and risk appetite and how does it influence the internal risk process ?”

Respondent : “Risk policy, appetite and culture that i mentioned before provides an umbrella framework for the risk governance body (i.e Executive committee) in doing the risk process.”

Author : “ Can you elaborate further on the risk process itself ?”

Respondent : “Basically the steps begin with risk identification, then risk assessment (assess the impact for the company), next step is risk mitigation (how to mitigate the impact and likelihood of the risk). Last step we monitor and make a documentation of it.”

Author : “So, basically these are the risk register, contains both top tier and bottom up risks.”

Respondent : “ Correct.”

Author : "Great. Now about the risk appetite. I noticed that the company put low rating on aspects such as compliance & legal; financial; client, products & market, based on legend, means that the company is very risk averse in most circumstances. Why's that so ?"

Respondent : "Yes, since we're the local subsidiary of a NYSE listed parent company, we are obliged to maintain a certain standard compliance of the imposed regulations. Failure to comply might have a severe impact to us as a global business."

Author : " What's the meaning of each level of risk appetite – low, moderate and high ?"

Respondent : "Low means we're very risk averse in most circumstances. Moderate means we're willing to accept risks once in a while and High means we're willing to accept risks in most circumstances."

Author : "I see. From your point of view, which risk(s) that are the most severe of all for local business in Indonesia?"

Respondent : "hmm.. i would go with error and ommissions. As a human consultant we are bound to do mistakes despite the fact that various controls and training efforts been made to encounter this risk. The likelihood is relatively moderate since doing mistakes are quite inherent as a human, compensated with experience, knowledge and training. As for the consequences, it could be severe. Imagine the damaged reputation, potential litigation, interrupted business & operations. Not a very keen imagination. You can see the details E&O in the documents i gave you previously."

Author : "What are the other risks that became your point of concern as well ?"

Respondent : “Well there are a lot of it. From legal side, besides E&O exposure, there’s compliance and inproper disclosure of confidential data risks. Eventhough we have give our best to comply and protect but to some extent, the risks are still there. From financial point of view, we are exposed to certain macro conditions of a country that we operate, the inable to recover during disaster also presented certain risk to us as a business and impacted PT XYZ financially. From competition point of view, we have a price conscious customer and generous competitors who will go to the extend of giving free services to lure PT XYZ customers. That’s tough.”

Author : “What about the high turnover in the past 2 years? I’m under the impression there’s a talent war in this industry.”

Respondent : “Yes, that’s risk too. Lately the high employee turnover gives management a hardtime to find successors, not to mention our loss when big client follow to move to employee’s new company.”

Author : “Related to your risk register that you provided previously, can you elaborate further on each item here?”

Respondent : “ It covers risks that i explained before. Also, there’s a risk relates to business interruption due to physical access limitation to Company. It’s inherent risk of doing business in this area near legislative building who oftenly get ambushed in demonstration activities. We also aware of the risk of loosing our assets, such as notebooks, data, money, and other assets. That’s why we have corporate security as rules of game on how to use our assets. You can see the categories here. There’s personnel risk that is emphasizing the importance of employee background screening. There’s also information security risk that brings many companies into data breach issue and being sued for that. There’s a cyber security risk are more to rules on how employees should use their internet priviledge (such as usage of email, websites, social networking, and so on). Cyber security risk are relevant to daily tools or applications that could be misused by unresponsible party for their benefit and our loss. Never underestimate external harddisk or flashdrive, those could be a virus container."

Author : "If the risk was that horrifying then what the company has done to mitigate the risk ?

Respondent : " We do have what we called as "Rapid Deployment Network Sensor Array and Monitoring Package or also called "SOC in a Box". IT colleagues could deploy it to identify potential threats."

Author : "In the event of data breach, what to do ?"

Respondent : "An immediate investigation and do remediation actions including informing the other party whose data been misused."

Author : "In the context of business model/change management mentioned in the risk register, what are the risks included there ?"

Respondent : "hmm.. PT XYZ has not yet found a strong business model, mostly due to competition pressure to give low pricing instead of premium service. We also not yet have a cross selling between department. Once it's up and running, i can imagine the potential additional revenue and growth that we can achieve in the future. And oh, Indonesia is a developing market. Not all of them realizes the true meaning of insurance for their own protection. Lack of awareness makes Indonesia still potential for growth and challenging."

Author : "Now, what about risks in compliance & finance ? Do you have any specific worries there ?"

Respondent : “I think it’s the same with any other companies whom worried of violations since the consequences can be damaging for business. PT XYZ tries it best to complied with applicable laws and regulation as much as possible. We have our legal and compliance team who devote themselves for this matter. For finance, as in any company our risks quite similar. It relates to forex exposure as we’re US based company operating in Indonesia, we have a bit issue on collection, and mis-manage cash flow effectively.”

Author : “ People are inseparable part of any company. What are risks for people ?”

Respondent : “Malfunction employees such as sick, injured or resigned employees/teams. There’s a time couple years ago, in which we lost most of a team due to hijjack by competitor. That business dept basically dying department when that happens. We learnt our lessons in hardway and pay more attention to our employees since then. Those are the most common risk that we face related to people.”

Author : “What about teamwork ?”

Respondent : “So far teamwork are not the issue. Employees are relatively professional despite their professional difference.”

Author : “Thank you. Now what about specific risk in IT ?”

Respondent : “hmm basically we have global and regional IT team who support us fully in IT related matters, including system application back up data, IT crash, IT infrastucture failure, upgrade system, etc. Almost all aspect of it. We maintain a minimum IT activities locally. Oh, i think one of the risk is related to our telecommunication. We are still using the old phone PABX system in which we can’t divert the phone, either to cell phone, or phones in other sites. Hence, sometimes clients complaint about us being so mobile and difficult to be contacted. From DRP point of view, this is also a risk since in case of disaster, we can’t directly divert our lines to the recovery site. But this our project, by the end of this year, the management approved to change the existing office telecommunication system. It was expected once the new system up and running, in business interruptions circumstances, telephone system will no longer be an issue. We can now automatically divert any incoming calls to our selected recovery site in case of disaster. The other thing that i notice is that the budget for IT tends to not be the priority as it perceived as having no direct contribution to increase company’s profit. But this should be a long term investment. Take the example of PT XYZ’s investment in Crime Prevention Through Environmental Design project. It is a way to deal with security issues.”

Author : “What about other IT risks?”

Author : “Can you explain about the implementation of Business Continuity Management in PT XYZ ?”

Respondent : “Yes, we do have Business continuity plan as evidence of BCM implementation. Take the file from my drawer.”

Author : “Can you please explain further regarding the plan?”

Respondent : “Well, basically our procedures are divided into 3 phases. One phase after the previous phase. The first phase is emergency response phase that is a phase where required an immediate respond when an event takes place. Country leader along with me will then discussed to assess the event. We’ll keep monitor the situation and determine whether evacuation is needed. If the situation is stable, we will draft a report to regional Business Resilience Management. And if not, we might need to move to the command centre (as part of Incident management phase). In this phase again we monitor the situation from command centre (which usually the house of one of the employees). If stable, we report. If not, the country leader will decide whether we need to proceed to the next phase, business continuity stage that is when we need to start all over again, pick up our resources, retrieve data, consider to use temporary premises, and various administrative staff. The most important is to maintain connectivity to our client, which means telephone, faxes, internet, emails are of the importance during these times and at best must be recovered first. These flowcharts might give to the big picture. You might put additional information that i gave just now."

Author : "What about your IT strategy practice ?"

Respondent : "These are the summary of our IT practices. You might add informations from my explanation, if any. Basically we'd like to protect our data as secure as possible, maintain client's trust by keeping their confidential data and adhere to the business continuity plan, including disaster recovery plan, as best as we can. These are some of IT security protocols such as password protected access control, accounts removal upon employee's move, encrypted data, building access is controlled according to each employees responsibilities, camera surveilance especially to monitor data areas including remote camera surveilance by authorized person, pre-approved system and configuration changes, firewalls, etc."

Author : "Any precaution actions in IT management to handle IT issues ?"

Respondent : "We do activate antivirus and antispyware programs, IT personnel monitor alerts from the system to ensure no violation in perimeters, a 24/7 global IT team to timely address IT issues, complianced with local regulations related to IT also crucial."

Author : “Is this an updated one ?”

Respondent : “No, it’s last year version.”

Author : “What happen to the new version ?”

Respondent : “There’s a delay in distributing this year updated BCP. But the substance of the contents remain the same. I have confirmed it with our regional and local BCM team”

Author : “Meaning all the team leaders and management are currently using the old version as their disaster reference ?”

Respondent : “ Yes”

Author : “Is there any definite/plan time as to when the updated file will be distributed ?”

Respondent : “No exact time yet.”

Author : “Does the BCP contains details of contact person of teams to be contacted in case of disaster ?”

Respondent : “ Yes, correct”

Author : “Our office is having a high turnover in the past 2 years especially in senior management / team leaders position, resulting in many position changes and i think the BCP should change as well to adapt these changes. Are we ready to face disaster just using old BCP contents that are not yet updated ?”

Respondent : “You’re right. We’re supposed to have the updated one as soon as possible.”

Author : “Thank you for your time and help. I’ll get back to you if i have more questions.”

Respondent : "You're welcome. Please have the company's name anonymous in your thesis."

Author : "I will."

APPENDIX 2

EXPLORATORY RESEARCH

Exploratory research : Interview with IT Department Head on 6 June 2011 to gain deeper understanding of existing disaster recovery plan of PT XYZ.

Respondent : IT Department Head

Author : "Good day Pak"

Respondent : "Good day, Siva."

Author : "As discussed during our meeting previously regarding today's interview agenda. I would like to elaborate further related to PT XYZ's existing disaster recovery plan in particular IT function."

Respondent : " Where do you want to start?"

Author : "I'll start with critical IT risks. What do you have in mind ?"

Respondent : " hmm.. current IT practices and control are quite strict and most of IT activities were performed by either global or regional team. I don't see any extreme critical IT risks leave unaddressed."

Author : "Can you please explain about our disaster recovery plan ?"

Respondent : "The program is part of the comprehensive Business Continuity Plan includes specific provisions during emergency response phase, incident management phase and business continuity management phase, such as staff mobilization, alternate work spaces, recovery of the local area network (LAN) and telecommunications, and communication with clients. These ns were created based on the Business Impact Analysis. It also address loss of office facilities, data, operating systems and/or application software, WAN/LAN services, and mission-critical technology infrastructure components. Plans also include procedures for appropriate data backup and retention in accordance with data retention policies, disaster impact assessment, time tables and action plans, coordination of national assistance, contingency plans to replace equipment, and to use other company offices and off-site recovery sites in the event of a loss of a facility. Plans are tested annually and updated as necessary to address deficiencies or identified gaps."

Author : " Do you have any documentation about DRP?"

Respondent : "I have this. Take a look if it's what you're looking for."

Author : " Yes, thank you. So what is the function of local IT team if most of IT activities were maintained by the regional ?"

Respondent : "Well, from the global point of view, centralized IT system with 24/7 supervision is cost efficient, improved control, faster respond as there's a dedicated and specialized IT team, centralized to address any issue globally. The local team is basically only maintain a server room that connects the network with PC's, Notebook's and printers. We also daily back up local server data into a media storage. This media storage is picked up by our vendor on every working day. It will then be stored in vendor storage room in Tanggerang. The vendor location is far enough but still within driving range of 1-2 hours. In emergency times to restore data, we're able to request the vendor to deliver the media data to the office. Just mention the tape number. Besides daily back up, we also do monthly back up. Daily back up tape usually will be override after 2 weeks period, but monthly back up data will be kept permanently in the vendor's storage for security reason. But this only applied to data put in server. For data inside system application, it will be maintained by the asia pacific regional IT team in Australia. Local team is working together with regional IT team. For example, when there's a virus attack few months ago, our regional IT team were able to detect the virus attack and within hours they asked the vendor to send the antivirus to Indonesia local office. Local IT team who was then do the field work cleaning up the infected computers. We are partners with the regional and global team."

Author : "How come we can be attacked by virus ? I thought antivirus already handled by the regional/global IT team."

Respondent : "After further investigation, it was due to one of employee was trying to instal a non-standard application into his PC (which contains virus). Since the PC is connected with the entire network, it exposes the whole system into malfunction due to virus. But luckily, our global team who already make an agreement with antivirus vendor are able to to provide the antivirus quickly. No damage noted."

Author : "What about the data backup?"

Respondent : "There are two types of data. Data from system applications such as Oracle, eGlobal, iMAP, etc. And the other is data located in local server (such as client data spreadsheet, scan files, . The first is being backed up automatically over night by the regional IT team to their storage on daily basis. The latter is being backed up by local IT team overnight too. In the morning, vendor picked up the media data

storage used to back up in the night to be kept in out of town storage place (Tanggerang). In addition to this formal data backup, i also do a personal backup in a special external harddisk. This harddisk is kept in house (in office) used for emergency data retrieval if needed. FYI. We also kept a special disk containing a standard image of every notebook or PC's in the company. 1 disk copy is kept in the office, 1 copy is kept by the IT Dept Head's home and 1 copy is kept by regional IT team. By keeping such imaging disk, in case of no notebook or PC's are working using the standard configuration, it could help formatting either the existing PC's or notebook or PC's or notebooks located in the recovery site. It’s being updated regularly to capture changes.”

Author :“How’s the maintenance of our server?”

Respondent : “Our server room has a specific room temperature and it has a limited access. Not all employees could go in and do whatever they want. The access is restricted to IT personnel only.”

Author :“Do we have emergency recovery site for IT ?

Respondent : “So far none, but we do have several preferred vendors. One is in Cikarang and the other one is in Jatiluhur. Both provides a full-equiped site such as workstations include tables and chairs, telephone lines, PC’s, a server room and even accomodation housing and food. The infrastructure also accomodates for connection between data centre of the preferred vendor and throughout the recovered data centre. If our end of year project go live, all calls through our new telephone system, could be diverted to this recovery site. Allowing continuance of our business operations.”

Author : “Do we have agreement with this preferred vendor ?”

Respondent : “No. I just did survey in the past just in case if we needed one. It’s part of our disaster recovery plan anyway. If the disaster effect only takes several days, we are bound to use conference rooms in hotels, but if the disaster takes longer time then there’s a possibility we need to move to this recovery site.”

Author :“What to do if there’s a software, applications and vendor performance failures ?”

Respondent : “The regional asia pacific IT team are in close supervision of software, applications and vendor performance. Any detected or potential issues are raised to the vendor by regional IT team for them to check and liaise further with respective party, if necessary. This is an IT risk that we need to watch out for.”

Author : “ So you’re agree that frequent failure in IT system will create certain IT risk for PT XYZ ?

Respondent : “Yes, of course.”

Author : “You’re mentioning about network. What’s the capacity of our network?”

Respondent : “Currently we have 1.56 Mb network bandwith capacity but the yearly utilization rate is high around 75%. See this online report. Indonesia is one of the country with the highest utilization in comparison with other brother companies.”

Author : “Will that cause a slowdown in the network ?”

Respondent : “Yeah.. several times, our system were down due to the limitation.”

Author : “Have we raised this issue to local management or regional team ?”

Respondent : “Of course. Talked to local management for approval.

Author : “PT XYZ is growing locally, the business is expanding, the number of employees also increased following such growth, meaning we will need additional network bandwith capacity to support our business. Slow system will not make things easier.

Respondent : “Agree on that. But all still in process.”

Author : “Thank you for the information. I’ll get back should i need anything else.”

Respondent : “No problem.”