BUSINESS CONTINUITY FOR DISASTER RECOVERY PLAN

SULIT SANGSUE

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE GRADUATE SCHOOL
STAMFORD INTERNATIONAL UNIVERSITY
MASTER OF BUSINESS ADMINISTRATION
ACADEMIC YEAR 2013

The Research has been approved by
The Graduate School
Stamford International University

Title: Business Continuity For Disaster Recovery Plan

Researcher: Sulit Sangsue

The Thesis Committee:

Chairman _____

(Assoc.Prof.Dr.Panarat Panmanee)

Advisor _____

(Dr.Ake Choonhachatrachai)

Committee Member _____

(Dr.Martin Goerlich **)**

Committee Member _____

(Dr.Puttithorn Jirayus)

_____

(Dr.Apitep Saekow)

Dean of Graduate School

January 2013

Title: Business Continuity For Disaster Recovery Plan

Researcher: Sulit Sangsue **Student ID**: 010270006

Degree: Master of Business Administration

Advisors: Dr. Ake Choonhachatrachai

Academic year: 2013

Abstract

The objectives of this study were (1) to examine the variable that has relationship for Business Continuity Management; and (2) to examine the differences between Business Continuity Management and its determinants.

Research Methodology**:** this research will be 400 both male and female, MBA or higher educated to understand business management term, aged between 20 year old to more than 65 year old people, who have work experience. Respondents came from Stamford International University (STIU), Ramkhamhaeng University, National Institute of Development Administration (NIDA), and Asian Institute of Technology (AIT). This respondent understand the concept of business continuity also work experience will help their answer the questionnaire

Research findings were as follows: the respondents more than half are female with total number 212 or 53% and the rest are male respondents of 188 (47%) making females the majority of the respondents of this questionnaire. The largest number of respond is Natural Disaster with a total of 304 persons (22%) the often of organization has interrupt their business that their organization thought. Most respondent answered"0-1 time" with number of 310 respondents (77.5%). Business Continuity Management is more and more important as business grow up relate to the study that nowadays there are plenty of book, case study, methodology, standard, and research on business continuity management. Therefore many organizations focus more on risk analysis and control then setup the policy and train their staff more often to avoid the risk such as fire training as standard twice a year. Testing power outage and start up power generator every one or two month for standby when the interruption come. The regression analysis shows the study of Business Management Continuity Management have relationships with Business Continuity Plan, Business Impact Analysis, Risk Analysis, and Testing and revising.

Keywords: Business Continuity Plan, Business Continuity Management, Business Impact Analysis, IT recovery plan

ACKNOWLEDGMENT

I would like to express my deep gratitude to Dr.Apitep Saekow and Dr.Ake Choonhachatrachai, my research supervisors, for their patient guidance, enthusiastic encouragement and useful critiques of this research work. I would also like to thank Dr.Dolly Samson, for her advice and assistance in my study.

Finally, I wish to thank my family for their support and encouragement throughout my study.

Sulit Sangsue

CONTENTS

CONTENTS (Cont.)

Page

LIST OF TABLES

LIST OF FIGURES

Page

CHAPTER 1

INTRODUCTION

This chapter presents the background of problems, main problems, sub-problem, and hypothesis, significant of the study, the scope and limitation of the study

1.1 Introduction

In the recent years, Disaster occur more frequent and more violent such as flood, airplane crashes and terrorist attacks are examples of man-made disasters: they cause pollution, kill people, and damage property.

The September 11 terrorist attacks in 2001 was a notable year for the world record, since then to still now people remember the terrific day of destruction, every year when September 11 comes, people do commemorate for recapture how insane terrorist attack was and how much sadness devastation has caused. This attack happened in New York and Washington, D.C., wherein 19 terrorists belonging to an Islamic terrorist group named al-Qaeda hijacked 4 airplanes. The first 2 airplanes collided into the World Trade Center, due to which these twin towers fell off within 2 hours and another attack was made on Pentagon building and one airplane got crashed in the fields in Pennsylvania USA. This incident took away the lives of nearly 3,000 people and caused heavy property and infrastructure damages of more than 10 USD billion. However, such attack demands re-considerations in policy making for health, law and order, cultural, and governmental relations. Also, there is special requirement to consider the business and economic aspect in such scenario. This can be one of example wherein the Business Continuity plan can be executed into the business plan to allow businesses to recover themselves.

Another example is the earthquake and Tsunami which caused Fukushima Daiichi nuclear disaster in Japan. On 11th March 2011 after the disaster, three of the six nuclear reactors of power plant were melted due to malfunction of reactor's cooling system and released substantial amount of radioactive material on 12 March. Around 300,000 people those who live within 20 Km area around power plant were evacuated and 15,884 people died due to the earthquake and tsunami. Fukushima

Daiichi nuclear disaster was measured Level 7 on International Nuclear Event Scale. This disaster is considered to be second largest nuclear disaster in world history after Chernobyl disaster in April 1986.

Thailand floods in 2011, was the worst flooding in the last five decades. It took nearly 6 months for disaster to end up. It started from late July until December and whole country suffered from it because floods started from Northern plain and spread out to Central plain along the Mekong river and the Chao Phraya river that are located in the heart of Thailand. 65 out of 77 provinces of Thailand were declared as flood disaster zones and over USD 45.7 brillion economic losses were estimated by World Bank. Flooding effect caused interruption in transportation mode in many of the important highways, lack of food, power outage and lack of communication throughout the country. In total, more than 884 people died and millions of residents were left homeless.

Nowadays, Information technology (IT) is playing as a key role for business. Over the years business had become dependent on information technology in every operation from the most basic thing to the most complex of operations. Information technology has great applications in almost all kinds of businesses which they are relying on computer for automating their traditional processes. Business use wide variety of database, management information system, information sharing, data sharing network, communication, internet, intranet, machine, equipment etc which highly rely on computer. The use of computer technology is not only for IT department but it is also being used by accounting & finance, marketing, human resource. Computer technology help to operate the routine business tasks much quicker as compared to the traditional way of doing things.

Without information technology or information technology interrupt the business can be disaster. Disasters can take several different forms. Some primarily impact individuals for example hard drive meltdowns while others have a larger, collective impact. Disasters can occur such as power outages, floods, fires, storms, equipment failure, sabotage, terrorism, or even epidemic illness. Each of these can at the very least cause short-term disruptions in normal business operation. But

recovering from the impact of many of the aforementioned disasters can take much longer, especially if organizations have not made preparations in advance. Disaster Recovery Planning is the factor that makes the critical difference between the organizations that can successfully manage crises with minimal cost and effort and maximum speed, and those that are left picking up the pieces for untold lengths of time and at whatever cost providers decide to charge; organizations forced to make decision out of desperation. Detailed disaster recovery plans can prevent many of the heartaches and headaches experienced by an organization in times of disaster. By having practiced plans, not only for equipment and network recovery, but also plans that precisely outline what steps each person involved in recovery efforts should undertake, an organization can improve their recovery time and minimize the time that their normal business functions are disrupted (DisasterRecovery.org, 2012).

After many experience of disaster, organization have think a disaster plan to ready for any disaster therefore become the words as we known as Business Continuity Management.

Business Continuity plan

A business continuity plan defines as "a set of procedures developed for the entire enterprise, outlining the actions to be taken by the IT organization, executive staff, and the various business units in order to quickly resume operations in the event of a service interruption or an outage". With markets being highly competitive as they are, an organization needs a detailed listing of steps to follow to ensure minimal loss due to downtime. This is very important for maintaining its competitive advantage and public stature (Wilson, 2000). The fact that the company's reputation is at stake requires executive management to take continuity planning very serious (IBM Global Services, 1999). Ensuring continuity of business processes and recovering the IT services of an organization is not the sole responsibility of the IT department. Therefore management should be aware that they could be held liable for any consequences resulting from a disaster (Kearvell-White, 1996). Having a business continuity plan in place is important to the entire organization, as everyone, from executive management to the employees, stands to benefit from it (IBM Global

Services, 1999). Despite this, numerous organizations do not have a business continuity plan in place. Organizations neglecting to develop a plan put themselves at tremendous risk and stand to loose everything (Kearvell-White, 1996).

Business continuity consists of the planning and management of contingency measures focused on the continued operation of critical operational business processes in the event of disruptions. Business continuity planning is a subcomponent of organizational contingency planning which is normally categorized as risk management. Contingency planning and management from an IT perspective includes Incident Response, Disaster Recovery and Continuity planning. In general, when one refers to Business Continuity Management (BCM) in an organizational context they are referring to the both planning and management. A formal definition is "Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities." (Reuvid, 2006). In some philosophies disaster recovery and business continuity are aggregated into the term business resiliency planning (BRP). This is synonymous with referring to BCM in most organizations. The similarity between disaster recovery planning and business continuity planning can introduce a high degree of overlapping, complimentary and seemingly ambiguous activities and concepts. The distinction between the two is disaster recovery is a completely reactive set of activities whereas business continuity planning is considered proactive set of activities (Glenn, 2002). Typically, BCM will nearly always involve some degree of movement of site operations to offsite facilities. Often the disaster recovery plan is incorporated into the business continuity plan and executed to some level, perhaps entirely in the offsite locations. In most modern enterprise IT equipment, a common feature for many technologies to include a High Availability (HA) configuration option. HA in principle implies redundancy. In many cases HA options include configurations that both improve and compliment disaster recovery efforts and subsequently business continuity process management (Lumpp, et al., 2008). However, HA/DR technology and configurations are also inherently more complex and increases the likelihood of human error contributing to IT

disruptions. One would be wise when planning and researching business continuity services to verify understanding and common definition of terms used in both documentation and discussions to remove assumptions on what terms like high availability mean to all parties.

Disaster Recovery Plan

Disaster Recovery Plan recently regarded as critical plan that prepared to face disaster or interruption which could impact our operations, services and as a result impact our reputation and people confidence. Disaster Recovery Planning is an effort to minimize the former, while maximizing the latter. According to survey by Patrowicz, 85 percent of the fortune 1,000 companies have disaster recovery plan. As cited in (Robbins-Gioia, 2003)stated that in a recent study by Gartner Group Research noted that approximately " sixty percent of business in the United States with reliance on IT infrastructure has not expended an adequate amount of resources for business continuity or disaster recovery. Furthermore, according to (Toigo, 2003) disaster recovery planning consists of a set activities aimed at reducing the like hood and limiting the impact of disaster events on critical business processes. Those, many organizations overlook the importance of DRP. Disaster Recovery Plan wills recovery from natural and human disaster such fire, software and hardware failure. The DRP is to ensure continuous support of its organizational goals and objectives. Disaster recovery is not just cover the equipment, hot site and materials, but it also represents communications, people interaction, and knowledge bases, strategy and backup (Colraine, 2005) Therefore, DRP does not have to be an elaborate framework of policies, procedures and hardware but much does in proper format. Without proper DRP, the lack of accountability, lack of coherent procedure, lack of standard documentation and effective communication will causes the loss of data and prolong plant shutdown

Moreover, Disaster Recovery Plan (DRP) itself obviously means planning how your business can recover to its former trading status if it should suffer some kind of major damage or other disastrous event (Paradine, 1995). This meaning was accepted by (Hawkins, 2000) when they say that Business Recovery Plan is the document used

to assist an organization in recovering its business functions. A Disaster Recovery Plan (DRP), however, is a document designed to assist an organization in recovering from data losses and restoring data assets. A Disaster Recovery Plan should be a pro-active document, a living and breathing document. It does not document the tasks, it is an action plan that is used to identify a set of policies, procedures, and resources that are used to monitor and maintain corporate information technology before, during, and after the disaster. (Ismail, 2005)

To conclusion type of disaster in the table will show two types of disaster which is natural disaster and man-made

Table 1.1 List of the disasters that can assail an organization

Natural disaster	**Man-Made**
Fires	Security incidents
Floods	Equipment failures
Tornadoes	Power failures
Hurricanes	Utility failures
Wind and ice storms	Arson
Severe storms	Pandemics
Wildfires	Sabotage
Landslides	Strikes and work stopping
Avalanches	Shortages
Tsunamis	Civil disturbances
Earthquakes	Terrorism
Volcanoes	War

Source: (Gregory, 2007)

Regarding the effects of disaster, business has to plan a strategy for business recovery and doing business continuity before disaster. The disaster can be any things, anywhere, and any time for example of big disaster in recent year and its effects.

Thailand Flood situation 2011

The 2011 flood of Thailand that was a very notable year in Thailand as the country endured enormous damage in the wake of the worst flooding in at least five decades. Throughout the entire calendar year, more than 884 people were killed and millions of residents were either left homeless or displaced following significant flooding. The most extensive flooding — and the primary focus of this report — occurred between late July and early December across nearly every section of the country. In total, 65 of Thailand's 77 provinces were impacted during this timeframe and damage was widespread and severe in many locations. Economic losses were estimated by the World Bank at THB1.4 trillion (USD45.7 billion), which makes the floods one of the top five costliest natural disaster events in modern history (Aon Corporation, 2011).

Table 1.2 Top 10 Natural Disasters in Thailand for the period 1900 to 2012 sorted by numbers of killed

Disaster	***Date***	***No Killed***
Earthquake (seismic activity)	26 December 2004	8,345
Flood	5 August 2011	813
Storm	27 October 1962	769
Flood	19 November 1988	664
Earthquake (seismic activity)	1 June 1955	500
Storm	3 November 1989	458
Flood	10 October 2010	258
Flood	3 January 1975	239
Flood	1 August 1995	231
Flood	20 August 2006	164

Source: (Centre of Research on Epidemiology of Disaster– CRED, 2012)

Table 1.3 Top 10 Natural Disasters in Thailand for the period 1900 to 2012 sorted by numbers of total affected people

Disaster	Date	No Total Affected
Drought	1 April 2008	10,000,000
Flood	5 August 2011	9,500,000
Flood	10 October 2010	8,970,653
Drought	1 March 2010	6,482,602
Drought	1 January 1999	6,000,000
Flood	30 June 1996	5,000,000
Drought	1 February 2002	5,000,000
Flood	1 August 1995	4,280,984
Flood	1 October 2002	3,289,420
Flood	3 January 1975	3,000,093

Source: (Centre of Research on Epidemiology of Disaster– CRED, 2012)

Table 1.4 Top 10 Natural Disasters in Thailand for the period 1900 to 2012 sorted by economic damage costs

Disaster	Date	Damage (000 US$)
Flood	5 August 2011	40,000,000
Flood	27 November 1993	1,261,000
Earthquake (seismic activity)	26 December 2004	1,000,000
Storm	3 November 1989	452,000
Drought	1 January 2005	420,000
Flood	1 December 1993	400,100
Flood	1 August 1978	400,000
Flood	19 January 1984	400,000
Flood	10 October 2010	332,000
Flood	31 October 1993	319,850

Source: (Centre of Research on Epidemiology of Disaster– CRED, 2012)

1.2 Statement of the problem

Natural Disaster is unpredictable that when it will come how damage it will take as Thailand face big flood in 2011 that was affecting every business over the country. Business face the interruption to operate the organization that organization was direct effect such as the work place flood, transportation and power outage. Economic losses were estimated by the World Bank at THB1.4 trillion (USD45.7 billion), which makes the floods one of the top five costliest natural disaster events in modern history.

As the result, the loss of business can be recovery faster or slow is depend on how organizations plan the Business Continuity. This research will focus on the factors that should be considered by the organizations for building Business Continuity Management effectiveness. Thus, the research problem is,

1. Is the effectiveness of business continuity management can bring back business faster?
2. Are there the relationships between IT Recovery and Risk Management in Business Continuity Management?

1.3 Objectives of the study

1. To examine the variable that has relationship for Business Continuity Management.
2. To examine the differences between Business Continuity Management and its determinants.

1.4 Scope of study

1. This study will examine various factors affecting business Business Continuity.
2. Respondents in this study will be 400 MBA or Ph.D. students from Stamford International University (STIU), Ramkhamhaeng University, National Institute of Development Administration (NIDA) , and Asian Institute of Technology(AIT).

1.5 Significance of the study

Nowadays, Business Continuity play important role after many organizations confront the interruption from disaster. As Recently, Thailand had been effect from big flood 2011, that most area of Thailand had been crisis from communication, transportation, power outage, infrastructure, and IT system. Although in core structure will be recovery by government but loss of reputation, customers, money, and database in computer are tragedy so Business Continuity plan, IT Disaster Recovery plan and employee reaction can make business faster recovery with less cost.

1. This research will help understanding variable that have relationship with Business Continuity.
2. This study will helpful for every organizations to appreciate important variable for prepare disaster plan

1.6 Definition of key terms

A **natural disaster** is the effect of a natural a hazard (e.g., flood, tornado, hurricane, volcanic eruption, earthquake, heatwave, or landslide). It leads to financial, environmental or human losses. The resulting loss depends on the vulnerability of the affected population to resist the hazard, also called their resilience. If these disasters continue it would be a great danger for the earth. This understanding is concentrated in the formulation: "disasters occur when hazards meet vulnerability." Thus a natural hazard will not result in a natural disaster in areas without vulnerability, e.g. strong earthquakes in uninhabited areas. The term natural has consequently been disputed because the events simply are not hazards or disasters without human involvement. A concrete example of the division between a natural hazard and a natural disaster is that the 1906 San Francisco earthquake was a disaster, whereas earthquakes are a hazard. This article gives an introduction to notable natural disasters, refer to the list of natural disasters for a comprehensive listing.

Man-Made is Anthropogenic hazards or man-made hazards can come to fruition in the form of a man-made disaster. In this case, "anthropogenic" means threats having an element of human intent, negligence, or error; or involving a failure

of a man-made system. This is opposed to natural disasters resulting from natural hazards.

Recovery Point Objective or RPO is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT Service due to a Major Incident. The RPO gives systems designers a limit to work to. For instance, if the RPO is set to 4 hours, then in practice, offsite mirrored backups must be continuously maintained- a daily offsite backup on tape will not suffice.

Recovery Time Objective or RTO is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

CHAPTER 2

LITERATURE REVIEWS

This chapter reviews the relevant literature related business continuity management which focus on how business can continuities when business face the disaster situation.

2.1 Concept of Business Continuity Management

Business continuity management consists of the planning and management of contingency measures focused on the continued operation of critical operational business processes in the event of disruptions. Business continuity planning is a subcomponent of organizational contingency planning which is normally categorized as risk management. Contingency planning and management from an IT perspective includes Incident Response, Disaster Recovery and Continuity planning. In general, when one refers to Business Continuity Management (BCM) in an organizational context they are referring to the both planning and management. A formal definition is "Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities." (Reuvid, 2006)

In some philosophies disaster recovery and business continuity are aggregated into the term business resiliency planning (BRP). This is synonymous with referring to BCM in most organizations. The similarity between disaster recovery planning and business continuity planning can introduce a high degree of overlapping, complimentary and seemingly ambiguous activities and concepts. The distinction between the two is disaster recovery is a completely reactive set of activities whereas business continuity planning is considered proactive set of activities (Glenn, 2002). Typically, BCM will nearly always involve some degree of movement of site operations to offsite facilities. Often the disaster recovery plan is incorporated into the business continuity plan and executed to some level, perhaps entirely in the offsite locations. In most modern enterprise IT equipment, a common feature for many

technologies to include a High Availability (HA) configuration option. HA in principle implies redundancy. In many cases HA options include configurations that both improve and compliment disaster recovery efforts and subsequently business continuity process management (Lumpp, et al., 2008). However, HA/DR technology and configurations are also inherently more complex and increases the likelihood of human error contributing to IT disruptions. One would be wise when planning and researching business continuity services to verify understanding and common definition of terms used in both documentation and discussions to remove assumptions on what terms like high availability mean to all parties.

Business Continuity Plan

The majority of organizations today realize that they cannot function without the continued availability of their information technology resources (McKinney, 2000). Therefore, they are constantly at risk due to the threat posed to their information by natural disasters and other unforeseen events. As they become more dependent on continuous availability of their information, organizations have to take measures to ensure that business continues as usual following some disaster or event (Underwood, 1998)

No organization is immune to the effect of disasters and these disasters might prove fatal to its survival. Fires, floods and explosions usually come to mind when the word disaster is mentioned, but virus infections, unreliable data, and hardware and software failures are, however, a more common occurrence. A large number of organizations affected by a disaster do not have procedures in place in order to effectively deal with it (Boddington, 1998). Therefore, companies may experience major survival threats if they do not have some form of continuity procedures in place to help them through the normalization period. In the past such procedures served primarily to ensure that the data center of an organization kept downtime to a minimum. These procedures to recover the data center were generally known as disaster recovery procedures (IBM Global Services, 1999).

As technology evolved and became more sophisticated, organizations started to rely a great deal on the availability of their systems and technology. As continuous availability was now important, Disaster Recovery Planning evolved into BCP. The aim of BCP is to make data center downtime transparent to those outside the organization (King, 2000). Many companies, especially those that are Web based, must operate twenty-four hours a days, seven days a week and BCP helps these companies to achieve a state of complete business continuity (IBM Global Services, 1999).

For many organizations the World Wide Web is increasing in popularity as a tool to conduct business. This unfortunately means that disaster tolerance and recovery is also growing in importance for these organizations. A disaster could mean that an organization would no longer be accessible to their customers, employees and suppliers. This could in turn mean major losses in income and valued customer support by (Florendo, Martens, Middlebrooks, Romanyschyn, & Solter, 1998)

Disasters and Business Continuity Planning

"A disaster may be any accidental, natural or malicious event which threatens or disrupts normal operations, or services, for sufficient time to affect significantly, or to cause failure of, the enterprise" (Hassim, 2000). Business disasters need not be to the extent of a hurricane to pose a serious threat to an organization.

Disasters are not bound to time or location either. The majority of disasters are as a result of unplanned events in and around the working environment. Such disasters could be as trivial as neglecting to save an important file, a complete network failure, losing installation backup disks or the loss of the original copy of an important document. They could furthermore include the compromising of an online transaction processing web site or the deletion of critical files by a new employee (Wilson, 2000).

Nowadays the outages caused by these risks are measured in hours and no longer in days. For e-business, it is more important to be able to handle sudden peaks in web traffic than worrying about natural disasters. Electronic transactions take place at an incredible rate. The work and business that could be done in an hour by far

exceeds that of previous decades. What was previously seen as a trivial event, for example a defective hard disk or a software malfunction, could today be seen as being of the same magnitude as effects caused by a natural disaster some decades ago (IBM Global Services, 1999).

The Evolution of Business Continuity Planning

During the 1980's a discipline known as Disaster Recovery Planning (DRP) was formally accepted and was aimed at protecting an organization's data center from the effects of disasters. The data center was central to the organization's IT based structure at the time (IBM Global Services, 1999). However, the IT environments at present differ from the host-centric systems of two decades ago. Networks are more complex and consist of several servers and a large number of personal computers and peripheral devices. Already in the early 1990's organizations started abandoning the centralized approach with the advent of distributed computing and client/server technology (IBM Global Services, 2000).

This shift in technology also brought about a change in organizational functioning. Information technology became intertwined with the majority of business functions. Information essential to business survival was spread across the organisation and not found only in the data centre anymore. Critical business functions continuously access this critical information on a regular basis. Information technology has, therefore, become a critical component of business. It is no longer enough to safeguard information only, but the critical business processes as well (IBM Global Services, 1999).

Business Continuity Planning Process

The Business Continuity Planning Process Business continuity planning should determine what impacts would be suffered by the organization if disaster-whatever its form - strikes. It should identify the critical business functions, and the critical resources upon which those functions depend. It should also determine the critical timescales for the recovery of those functions, in order of priority (Smith & Sherwood, 1995).

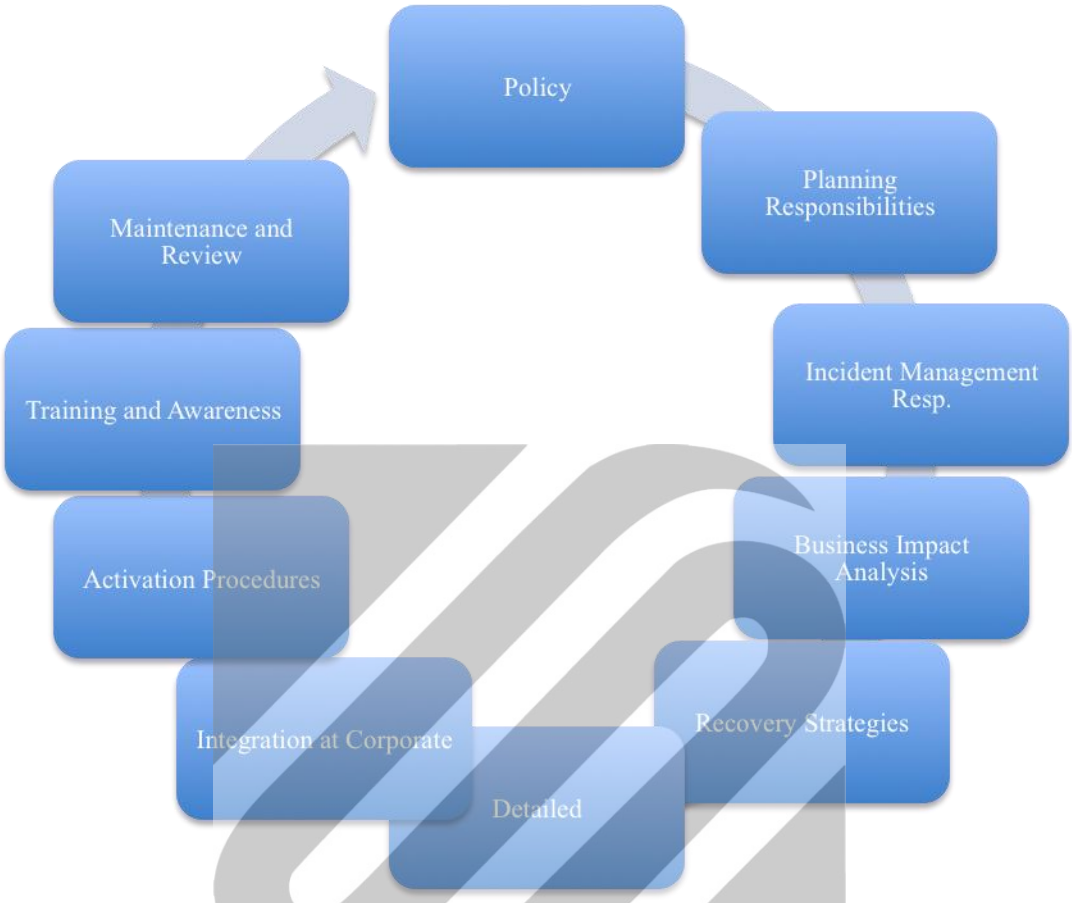

Figure 2.1 Business Continuity Planning Process

Source: (Smith & Sherwood, 1995)

Risk Analysis

The purpose of the risk analysis phase is the identification of procedures that, if carried out, could possibly prevent or reduce the effect of a disaster. These procedures include educating personnel about issues such as security, vandalism, workplace violence etc. A risk analysis exercise also involves the analysis of the organizational environment to identify threats that could lead to a disastrous situation. Areas to be reviewed for such threats are the actual physical location of the organization, access security, the organization's policies and practices and the construction of any of the organization's facilities. The objective is to identify the vulnerabilities that could cause the most damage to the organization and to select the appropriate controls for providing effective protection (Roberson, 2000)

Business Impact analysis

The business impact analysis phase would involve the identification of the functions most critical to ensure business continuity as well as the time frame and required resources for each function. The reason for doing this is to develop an effective recovery strategy. This is done by reviewing these functions and prioritizing them based on each function's recovery time frame. The Business Impact Analysis study has to gather information about vital records, systems control methods and the current recoverability of the organization. Organizational procedures are also reviewed and if necessary, improvements are suggested (Roberson, 2000)

The business impact analysis phase involves identifying those business processes most critical to the organization, establishing the recovery time for each function and determining what the financial impact is that these functions may have on the organization. The critical systems, processes and functions must be identified along with the economic influence of disasters on each. The amount of time each business area is able to function effectively without access to critical systems and services should also be identified. Lastly, the recovery timeframes for critical systems must be determined as well. Devargas (1999) mentions that the deliverables are a business impact analysis report, a risk assessment review and business continuity plans.

As planning for the BCP project has now been completed, the next logical step is to identify and then analyze the business processes that are critical to the organization. This is done through a Business Impact Analysis (BIA). The aim is to separate those processes without which the organization cannot function as usual from those that are less important or even redundant. An analysis of each process should include the identification of all costs emanating from the inability to complete the process, because of some disaster or event, as well as the resources required by each (Wilson, 2000).

After the analysis of processes, they are generally prioritized by means of a predetermined ranking system. The maximum amount of time each can be unavailable before business is impacted is also determined during the BIA. Once this has been

done it is possible to understand the impact that various disasters may have on business (Gordon, 2000) The rest of this section will, therefore, discuss the process of performing the BIA. Specific steps will include the identification of critical business processes, identifying various disaster scenarios, determining the various costs involved, prioritizing the critical processes and determining which resources are critical to each process. It must be indicated that none of the steps discussed below have been found to be directly influenced by the identified SME characteristics.

IT Recovery Plan

IT Infrastructure recovery

The IT recovery plan phase contains all the tasks necessary to be completed in order to fully recover the data center. These include activities usually forming part of a conventional disaster recovery plan such as the recovery of all systems and applications needed by the various business functions (Roberson, 2000)

This phase also defines and implements the necessary tasks to fulfill the recovery strategy requirements. If the recovery strategy specifies a hot site for the data center and a work site for a specific number of personnel, then the resources to make this possible must be acquired somehow. If a vendor will be used the vendor would need to provide for both these strategies to be implemented and still be competitive in terms of pricing and conditions. The vendor should also be able to provide for unique technology requirements (Roberson, 2000).

Recovery Time and Point Objectives

The Recovery Time Objective (RTO) refers to the maximum amount of time a process or system can be unavailable for. If the RTO is large, the less it will cost an organization. In other words, the longer the RTO, the larger the costs incurred due to the unavailability of the process (Lapedis, 2001). Each business process needs to be examined and assigned an RTO. To accomplish this, both managers and staff involved in each process need to agree on this assigned value. The length of the RTO depends

largely on how keen employees are to find alternatives for continuing each process (Button, 1995). A further factor that needs to be identified for processes is the Recovery Point Objective (RPO).

RPO is a factor indicating how current a specific data set is and needs to be determined for all data. This value needs to be identified if a suitable backup method is to be chosen. If the data should not be more than four hours old, for example, before the disaster occurred, one should choose the appropriate backup method or technique (Gordon, 2000).

Only using the RTO and RPO as prioritization values are however not sufficient. Though some business processes might not need to recover as quickly as others, it does not mean that they are not critical. Therefore, the cost of the impact on each business process needs to be taken into consideration as well as to determine the criticality factor of each process (Button, 1995). Therefore, the next sub- section will identify the various costs that need to be identified for prioritization purposes.

Many organizations put the cart before the horse in selecting and deploying technologies before understanding the business needs as expressed in RPO and RTO; IT departments later bear the brunt of user complaints that their service expectations are not being met. Defining the RPO and RTO can avoid that pitfall, and in doing so can also make for a compelling business case for recovery technology spending and staffing (Levine, 2009)

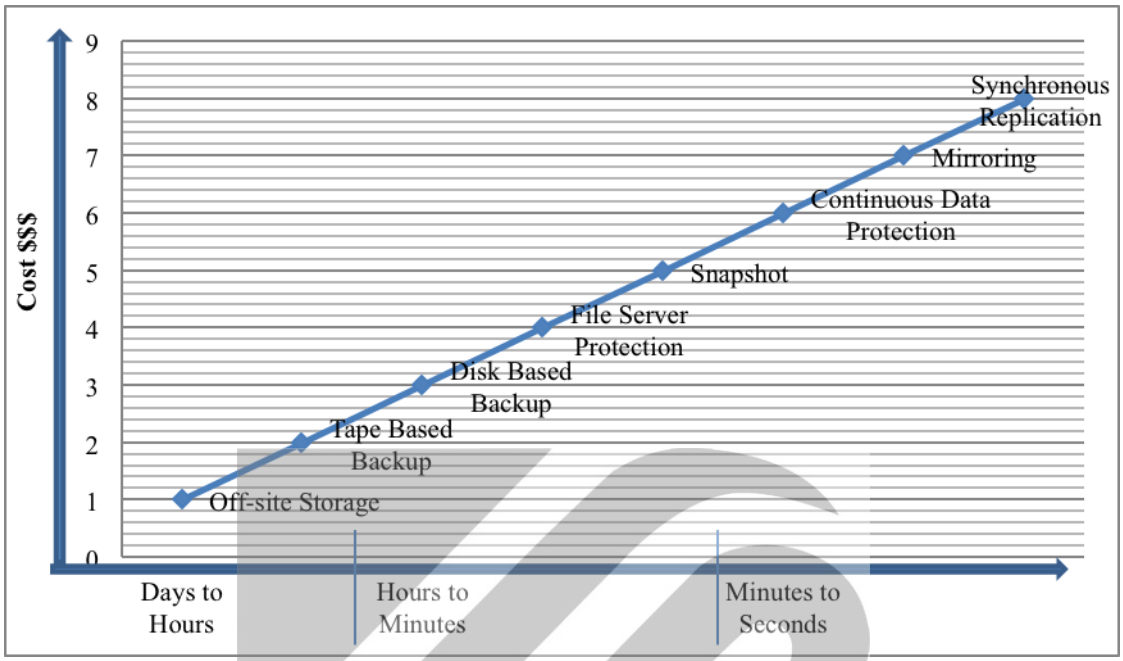

Figure 2.2 Data Recovery Continuum of Service

Source: (F5 Networks Inc., 2012)

The RTO is the maximum allowable downtime after an outage for recovering systems, applications, and functions (see Figure 2.2). RTO provides the basis for developing cost-effective recovery strategies and for determining when and how to implement these recovery strategies during a disaster situation. **The Disaster Recovery Continuum of Service – The Faster You Want Data Back, The More You'll Pay –** The recovery point, for example, defines how current the data is after a disaster. The RPO is the earlier point in time to which systems and data must be recovered after an outage. RPO defines the maximum amount of data that your organization is willing to sacrifice after a disaster; i.e. a zero RPO business continuance solution can survive a disaster without any loss of data.

Together, RTO and RPO provide a measurable target for your business continuance and disaster recovery solution to achieve. Improving RTO and RPO requires increasing your investment in networking and storage technologies and processes. Also, the physical distance between your data centers and how well your applications tolerate network latency affects how close you can get to zero RPO. That

is why you should limit your RTO and RPO to whatever levels your organization can effectively tolerate (F5 Networks Inc., 2012).

Data Recovery

Ensuring continuity of business processes and the recovery of the IT department are almost physically impossible without data. Therefore, if an activity has to be chosen as a first step towards a recovery plan, it is the backing up and protection of an organization's critical data (Koski, 2001)

Tydlaska (1996) said a good backup plan should thirdly generally include procedures that specify the backup frequency of identified data. Such a plan should furthermore specify who will be performing these backups and where they will be stored Also, he considerate the amount of copies that are to be stored of the backed up data. More than one copy should also exist, preferably three according to industry standards.

Goggins (1996) considerate that the data should be easily obtainable in event of an emergency and it should be specified who is authorized to retrieve the backups. Furthermore, the time it will take to retrieve the data must also be determined. Also, the amount of time it will take to restore the backups must be determined and the person(s) responsible for data restoration must be identified.

Once all data is backup up, it needs to be securely stored for swift recovery during disaster situations. Typically, an offsite location needs to be far enough away not to be affected by the disaster as well. An increase in distance does, however, increase transportation costs (Larue, 2000). Transportation of backed up data can be carried out physically or electronically. When physical methods are used, the organization is responsible for delivering the data to the offsite location themselves, or they could make use of overnight carriers. The drawback of overnight carriers is that it can become less cost effective as the amount of tapes to be delivered increases. An organization could also make use of an offsite storage vendor. In this case the vendor is responsible for managing the backup transports and archiving. (Larue, 2000)

The drawback of this approach is that it could be very expensive for smaller organizations. Organizations can, however, be certain that backups are handled professionally if they use this approach (Gulley, 1999). Data can also be transmitted electronically to the offsite location by means of electronic vaulting. Depending on the type of connection used, this approach could be very costly. A dedicated line would ensure swift backup and recovery of data, but could prove expensive. Another option is sharing a connection or making use of a smaller line. Unfortunately the drawback then is the data transfer speed and the recovery time (Gulley, 1999).

If the continuous availability of an organization's data is of utmost importance they can also consider mirroring the data on an identical system. Therefore, organizations must evaluate the recovery windows and how critical the data is when choosing an approach (Hurwicz, 2000). Financial performance and SME budgetary issues are bound to play a role when it comes to choosing an appropriate backup strategy.

- **Hot Sites**

Hot Sites are probably the ideal situation where redundant systems, applications and infrastructure that mirrors existing production systems are already in place and functional and where only data transfer and personnel need be relocated. It offers a perfect environment to test and verify and prepare. In some cases the hot site may serve as the remote backup or disaster recovery location(s). Few organizations have the resources to make this option a reality. The recovery time could be as little as several minutes to several hours. With this option, the major expenditure occurs prior to the disruption (Peterson, 2009)

- **Warm Sites**

Warm sites are a step below in equipment and capability of a hot site. The definition of warm site will be slightly different for each one but normally they will offer similar infrastructure and key systems, and will require configuration to become operational. Similar to the hot site option this is also an expensive option for most

organizations. Recovery time may be several hours to several days. With this option, the expenditure is disbursed more evenly through the process. (Peterson, 2009)

- **Cold sites**

Cold sites are characterized by the minimization or perhaps nonexistence of infrastructure systems. They are typically an empty office/warehouse space. However, this option may be all certain organizations or functions would require. Realistically, the cold site option could take days to weeks to provide a viable recovery of operations for most organizations. In this strategy the expenditure is primarily realized during the restoration process. (Peterson, 2009)

Project Planning

The project planning phase attempts to verify the scope of the business continuity project. This includes setting up project schedules, determining what needs to be done and identifying factors that could delay the project or influence its success. The phase also involves appointing a decision board whose responsibility would be to guide all participants in the planning project and to give some direction to the project. Another task that needs to be completed during this phase is setting up schedules for conducting the Business Impact Analysis. According to Devargas, the deliverables of this specific phase are senior management commitment, the project infrastructure, project plans and awareness campaign plans (Devargas, 1999).

The most important step in the project planning phase is to obtain senior management commitment. The fact that senior management acknowledges and accepts the BCP project is imperative to ensure success. Pre-project planning, which serves as preparation for the planning phase, should also be done. These activities would typically include the negotiations with relevant parties to ensure the availability of the required resources. It would also include combining collected planning information and appointing a manager to oversee the BCP project (Heng, 1996).

Vulnerability Assessment

Vulnerability assessment phase During the vulnerability assessment phase all, or most of, the factors that could affect the completion of the business processes are identified. Business areas such as personnel, communications, operating procedures, backup and contingency planning, data, systems, access control and insurance should be reviewed for this purpose. Deliverables for this phase include assessment reports consisting of a worst-case scenario and recommended scenario, as well as a business health check report (Devargas, 1999). A business health check generally involves an operations audit to ascertain whether operations are performed as efficiently and effectively as possible (Scheur Management Group, 1999).

Strategy Development

The strategy development phase aims to review the different options available for recovering those critical business processes as identified in the previous phase. An attempt is made to develop a collection of recovery alternatives as well as the operation plan that follows. Distinction is made between outages ranging from short to long term. The implementation of the recovery plan includes effecting changes to all procedures, negotiating contracts with recovery services vendors and defining recovery process teams. The tasks to be completed by these teams should also be defined. Deliverables include the disaster recovery procedures and training plans (Devargas, 1999).

Testing/Exercising Program

During the testing/exercising program phase, the objectives and strategies for testing the developed continuity plans are identified. The organizational needs and culture play a big role in accomplishing this. These aforementioned objectives need to be agreed upon by all participants, but as soon as this has been done the tests can be developed and carried out. Once completed, the tests results can be evaluated. Deliverables include the results from the four types of tests (Checklist, Simulation, Parallel and Full interruption tests), business continuity tests plans, a risk assessment review and contingency options report. The last two deliverables are included as

addendums to the plan (Devargas, 1999).

Testing Having reviewed various different methodologies, it has been noted that most other methodologies tend to combine the testing, training and maintenance phases to produce a single phase. The bank has, however, decided in their methodology that the training should be conducted as part of the testing. They do not, however, combine the two activities into a single phase, because during the second cycle of testing each of these phases has its specific purpose (Heng, 1996).

Maintenance Program

In order for the continuity plan to reflect the ever-changing organizational needs, they have to be updated whenever necessary. Any change management procedures should be carried out in view of the developed recovery plan. The only deliverable for this phase is the business continuity plan (Devargas, 1999).

Recovery Strategy

The recovery strategy adopted by the current methodology is categorized according to the length of business function recovery windows. These categories are pre-stage, subscribe and acquire. The pre-stage category is used for recovery windows of minutes to a few hours. It involves pre-planning for the critical resources that could include a fully operational and redundant data center, carrying out the necessary critical operations or just switching incoming calls to a redundant call center. The subscribe category is used for recovery windows of twenty-four hours to a couple of days. During this time recovery service vendors are usually used to recover the data center or workplace. The acquire category is used when the recovery window ranges from a couple of days to several weeks. The assumption made for this category is that all required resources would be purchased, rented or leased once the disaster has occurred (Roberson, 2000).

Recovery Strategy During the recovery strategy phase the users are allowed to methodically analyse the recovery process without actually writing detailed recovery procedures. All the work completed in this phase allows users to visualise the organisation's approach to recovery and continuity. The phase also includes discussions with the appropriate authorities and the parties involved in the project before any effort is made to develop the necessary recovery procedures. The recovery strategy phase includes the development of strategies for recovering the business functions and IT department, backup procedures, identifying the minimum processing required and determining alternatives for processing recovery (Heng, 1996).

Enterprise Solutions Study

The enterprise solutions study phase entails implementing the solutions as developed during the recovery strategy phase. The critical functions are prioritised during the Business Impact Analysis phase and the developed plan will show the path followed to develop the required solution. The size of the projects at this stage is dependent on how much the current recovery capability differs from the desired recovery state. The plan timeframes will also depend on the difference between how much is spent on plan development and how much the organisation stands to lose if business continuity is affected (Roberson, 2000).

Plan development

The Standard Chartered Bank makes use of continuity planning software to assist with the development of the business continuity plan. An important consideration during this phase is training users on how to use the software. The templates that form part of the software also need to be customized before any of the plans are created using the software. The plan includes stages such as emergency response, business and report functions recovery planning, the recovery process and returning home (Heng, 1996).

Identifying mission or business critical functions

Ensuring the continuity of business processes can prove difficult if they are not clearly identified. It is essential that managers understand the organisation from a viewpoint that is wider than what they are used to. A business plan, which is the definition of the critical functions of an organisation, needs to be developed. This plan not only identifies the functions but prioritises them as well. It could happen that in the event of a disaster certain procedures will not need to be carried out. If the priorities for each business function have been set and have been approved by management it could play an important role in determining whether the organisation will survive a disaster (Guttman & Roback, 1995)

Identifying resources supporting critical functions

Once the mission critical functions have been identified, the resources supporting these functions should be identified along with their usage timeframes. The effect that unavailability of these resources would have on the function should be determined as well. Identifying the resources is, however, not an easy task. Departmental managers regard some resources as important and could overlook others. Those individuals who understand how functions are performed should therefore analyse resources and interdependencies. This would simplify the prioritisation of identified resources (Guttman & Roback, 1995)

Anticipating contingencies

Identifying all possible events that could affect the normal day-to-day functioning of the organisation could prove difficult. By doing this the organisation can use the developed scenarios to develop a plan that will cater for a wide range of disasters. The developed scenarios should include both small and large disaster situations. They should also include all the resources as identified in the previous step (Guttman & Roback, 1995)

Selecting Contingency Strategies

Once the various scenarios have been developed, it is time to start planning for the recovery of required resources. When considering the alternatives one needs to take into account the controls that are in place in order to prevent or lessen the effect of disasters. Seeing that no collection of controls can prevent all possible disasters in a cost effective manner, the necessity exists to coordinate the prevention and recovery efforts (Guttman & Roback, 1995)

Implementing Contingency Strategies

As soon as the development of the recovery strategies have been completed, it is time to implement these strategies, document them thoroughly and the train employees (Guttman & Roback, 1995)

- **Implementation**

Much preparation is needed when wanting to implement the developed strategies. One needs to, for example, set up procedures for backup as well as contracts and agreements. It would be necessary to negotiate existing contracts to make way for new services. This preparation would also involve assigning personnel to various tasks should disaster strike. The team to perform these tasks is often called the emergency response team.

- **Documenting**

The documenting step involves the actual writing of the plan. The plan also needs to be maintained after any changes occur in the organization and its systems. It needs to be well written in case of the unavailability of critical personnel. Tasks should be simple and clearly stated in order for someone with minimal knowledge and experience to be able to perform them effectively. More than one copy of the plan should also exist and stored safely for redundancy purposes.

It is important that all employees involved in contingency planning should be well trained in performing their duties. As soon as new personnel join the organization

they also need to be made aware of their responsibility towards continued operations.

Testing and revising

A contingency plan will undoubtedly contain flaws and should therefore be tested vigorously in order to identify and correct these flaws. The plan will also become outdated as the resources supporting the critical functions change. One or more individuals should be made responsible for keeping the plan current. Various types of testing exists including reviews, analysis and disaster simulations (Guttman & Roback, 1995). A review simply involves testing the contingency plan regarding its accuracy. This would, for example, include checks to determine if employee listings are current and that tasks assigned to them are still the same A plan analysis is usually done by an individual not directly involved in the development of the plan but still has a good working knowledge of the different business functions and the resources supporting them. The plan is analysed by mentally following procedures stated in it in order to identify mistakes in the logic thought processes of the developers. The entire plan can be analysed at once, or only part of it if desired A disaster simulation is a valuable tool for identifying flaws in the plan, as well as assisting employees to practice for actual emergencies. These tests assist in providing important information for assuring business continuity. They are, however, expensive to conduct. A rule of thumb is that the more important a function is to the organisation, the more cost effective it is to perform these simulations (Guttman & Roback, 1995).

2.2 Related Article and Research

Mick Savage (2002) publish article with Emerald on business continuity plan after the 11 September tragedy in the USA has provided a wake up call to remind businesses of the need for adequate disaster recovery and business continuity planning. A business continuity plan must be comprehensive and up to date.

The “plan” that results from BCP is important but the really important part is the process of creating the plan. It is here that the serious thought about the business and possible effects of a range of emergency incidents is carried out. This process results in “the plan” and involves such activities as business risk and impact analysis,

documenting activities necessary to prepare the organization for possible emergencies including strategic recovery measures, identifying and authorizing detailed activities for any disaster recovery phase, identifying and authorizing detailed activities for managing the business recovery process, testing and auditing the business recovery process, training staff in the business recovery process, and implementing a process for keeping the plan up to date.

Mick Savage article has only shows what variable that need to do or plan for disaster however, the article was not list about IT recovery in core variable however in year of 2000 J. Roberson in personal communication review his methodology the consist of a risk analysis, business impact analysis, recovery capability assessment, recovery strategy, enterprise solution study, business continuity plan and IT recovery plan. However, the year 2009 Christopher A. Peterson developed framework form Jonathan 2006 to have Risk Management, Business Impact Anaylsis and Business Continuity Plan

Preetish Ranjan, Prabhat Kumar, and Kumar Abhishek in 2012 were research on Business Continuity Planning in Indian Perspective. Business Continuity can simply be defined as: to identify critical business operations, to identify risk associated with those operations, to identify ways to mitigate or avert the risk, a plan to proceed business operations in event of emergency of disaster, a plan to rejuvenate business again as soon as possible.

The research study five major sectors operating in India i.e. Banking, TMT (Technology, Media and Telecommunication), FSI (Financial Services & Insurance), Manufacturing and Others (includes Educational Institutions, Non-Government Organizations, Research Institutes etc).

This indicates that in spite of being defined by regulatory authorities to have a BCM in place only 1/3rd of Banking Sector are fully prepared and rest are either partially prepared or not prepared at all. TMT sector proved to be a better sector than all others where almost 2/3rd of the organizations are fully prepared with a BCM plan in place.

This study implies that more than half of organizations are not ready for disaster. As researcher see the important of Business continuity Management that less organization understanding how important they are.

2.3 Research Framework

In this part of the study, the researcher shows the theories from the literature review to develop the conceptual framework of the research. This chapter comprises of four sections that are theoretical framework, conceptual framework, research hypotheses, and operationalization of related variables that are the examples of all variables and its sub-variable translated into action.

2.3.1 Theoretical framework

Methodology of Devargas

"Survival is Not Compulsory". There are comprises of six separate phases, namely the project planning, vulnerability assessment, business impact analysis, strategy development, testing and exercising, and maintenance phases. The methodology includes a component in the methodology that will help assess the health of the organization with respect to information security. This component is the business health check report, one of the deliverables of the vulnerability assessment (Devargas, 1999).

This report is the outcome of studying business areas such as backup and contingency planning procedures, insurance cover etc. The report could help to convince management and shareholders of the shortcomings of information security in the organization.

Methodology of J. Roberson

The IBM Business Continuity and Recovery Services Consulting Methodology consists of seven phases or components. These are: a risk analysis, business impact analysis, recovery capability assessment, recovery strategy, enterprise solution study, business continuity plan and IT recovery plan. Besides this, the entire methodology is further divided into three stages namely analysis, design and implementation

(Roberson, 2000). Most conventional continuity planning methodologies contain only a plan development phase or strategy implementation phase.

This methodology lacks a project planning phase. The project planning or initiation phase usually includes all activities that need to be completed in order to initiate the BCP project (Heng, 1996). These include steps such as obtaining senior management support, defining the planning responsibilities, deciding on the projectinfrastructure, setting up schedules for interviews to assist with the BIA, etc. (Devargas, 1999).

This methodology unfortunately does not include a testing phase. It is essential that business continuity plans are tested thoroughly to ensure that they are not flawed This would also allow employees and everyone involved in carrying out procedures stated in the plan how to react in the event of a disaster (Morwood, 1998). A separate testing phase is therefore required in the plan. During this phase testing objectives are established, the scope of the tests are determined and the results of the tests are evaluated (Smith & Sherwood, 1995)

Methodology of Heng

The "Developing a suitable business continuity planning methodology" and was developed for the Standard Chartered Bank of London. The methodology was completed after several conventional frameworks and methodologies had already been reviewed and adapted to suit the bank's environment (Heng, 1996).

This methodology combines the training and testing phases (Heng, 1996). Business continuity testing is an excellent learning experience for those involved in the planning project. It saves time by not physically having a training phase prior to testing. It furthermore allows better understanding of all recovery procedures by physically carrying them out during an exercise.

Methodology of the National Institute of Standards and Technology (NIST)

NIST is responsible for computer systems technology in the United States Federal government. Their goal is to develop standards and guidelines, provide

technical assistance and to research computer and telecommunications systems to effectively utilize Federal information technology resources. The methodology consists of six phases. These are identifying the mission critical functions, identifying the supporting resources, anticipating disasters, selecting contingency planning strategies, implementing contingency strategies and testing and revising strategies (Guttman & Roback, 1995).

The implementing contingency strategies phase found here can be seen as the equivalent of the plan development phase found in other methodologies. As pointed out in some of the previously discussed methodologies, the presence of a plan development phase is more effective if not combined with the strategy development phase. This allows plan developers to concentrate on each phase separately, and thereby developing more detailed strategies and a detailed recovery plan.

Methodology of Christopher A. Peterson

Business continuity consists of the planning and management of contingency measures focused on the continued operation of critical operational business processes in the event of disruptions. Business continuity planning is a subcomponent of organizational contingency planning which is normally categorized as risk management. Contingency planning and management from an IS perspective includes Incident Response, Disaster Recovery and Continuity planning. In general, when one refers to Business Continuity Management (BCM) in an organizational context they are referring to the both planning and management. A formal definition is “Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.“ (Reuvid, 2006) Figure 2.3, shows a diagram model of the major logical components of BCM, logically the process flows from Risk Management to a business impact analysis and a plan is formulated primarily from these two inputs combined with other business objective requirements. (Peterson, 2009)

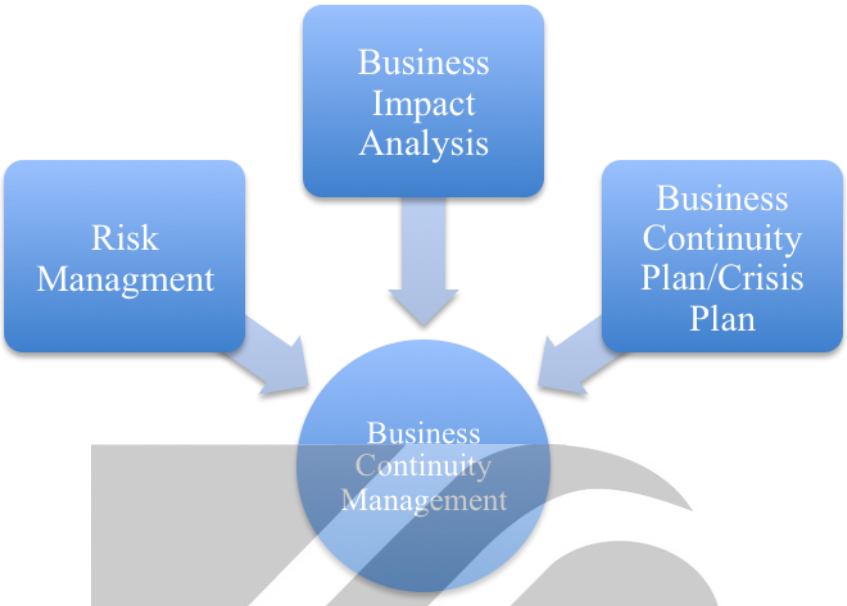

Figure 2.3 Business Continuity Management Model

Source: (Peterson, 2009)

2.3.2 Conceptual Framework

Review of the related literature and studies, the researcher drew a conceptual model as show in Figure 2.4 of how one theorize the relationship among several factors that developed from Christopher A. Peterson in year 2009 that include Business Continuity Plan, Business Impact Analysis, and Risk Analysis. However, researcher adopt conceptual more to have IT Recovery from J. Roberson in personal communication from year 2000 also J. Roberson framework include Risk Analysis, Business Impact Analysis, and Business Continuity Plan as well. However, Testing and Revising from Guttman & Roback in the National Institute of Standards and Technology (NIST) from year 1995 also need to be core variable for business continuity management to make the plan up to date.

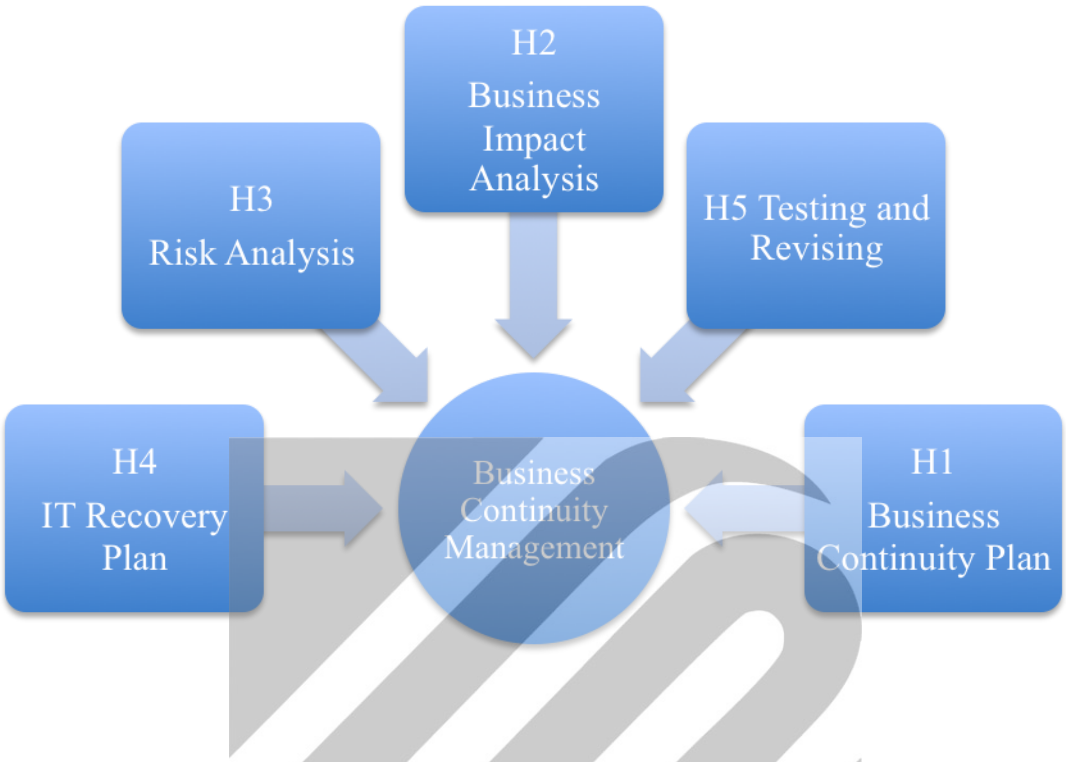

Figure 2.4 Conceptual model of Business Continuity Management

2.4 Hypotheses

The research hypotheses are presented in their null and alternative forms, as follows ,

H1₀ Business Continuity Plan will have no positive direct effect on Business Continuity Management.

H1₁ Business Continuity Plan will have a positive direct effect on Business Continuity Management.

H2₀ Business Impact Analysis will have no positive direct effect on Business Continuity Management.

H2₁ Business Impact Analysis will have a positive direct effect on Business Continuity Management.

H3₀ Risk Analysis will have no positive direct effect on Business Continuity Management.

H3₁ Risk Analysis will have a positive direct effect on Business Continuity Management.

H4₀ IT Recovery Plan will have no positive direct effect on Business Continuity Management.

H4₁ IT Recovery Plan will have a positive direct effect on Business Continuity Management.

H5₀ Testing and revising will have no positive direct effect on Business Continuity Management.

H5₁ Testing and revising will have a positive direct effect on Business Continuity Management.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter is focus on the methodology that was applied in this study. There are 5 sections in this chapter which is research design which is show how this study selected the information to design the research. Next section is construction of questionnaire that show how to construct the most effective of the questionnaire to find the answer in this study. Third section is actual questionnaire that will be use to survey. Fourth section is sampling and procedure that explore how this study use sampling to get the answer. The last section is data analysis that show how to analysis the overall data to get the final result of the study.

Both primary and secondary research were applied to achieve the aim and objectives of this study. Secondary research was use to generate the background of business continuity concept in term of literature review while survey was use as primary data to develop disaster recovery plan. Research design and detail of questionnaire together with sampling and procedure were presented in this part

3.1 Research Design

As this research aims to study the concept of business continuity plan toward both primary and secondary research to fulfill the data to complete its aims. Saunders et al. (2003) support the information that collected from primary research will provide in-depth and updated data. Also, secondary research provide a helpful source to answer a research question. According to Malhotra and Birks (2005) explain secondary data as data collected for some purpose whereas primary data are data originated by the researcher specifically to address the research problem. Some research use only one type of data whilst others suggest that both types may be appropriate (Hyde, 2000). To find out the effectiveness of business continuity, it may be advantage to use a primary data to show the real statistic. However, secondary data provide a basic knowledge that enables the researcher to understand the relating theories in literature.

Secondary Research

Secondary data provide high quality data for researchers. Saunders et al. (2003) claim that secondary research carries both quantitative and qualitative information, that includes raw details and published summaries, and most organizations collect and store a variety of data to support their operations.

The secondary, sources for this study contained academic books, journal, and articles, in this dissertation was presented in the form of literature review in order to build the arguments from business continuity and disaster recovery concept also used to support the finding of the primary research

Primary Research

This research consists of questionnaire which is a helpful method of accessing information business continuity about what respondents think in business continuity also their experience how organization effect from last disaster or how they plan it. Saunders et al. (2003) define primary research as being the most update way to find or look for the answer by recording, description, analysis and interpretation of people's behavior. The primary information was obtained from questionnaires which were passed out to the MBA or Ph.D. students from Stamford International University (STIU), Ramkhamhaeng University (RU), National Institute of Development Administration (NIDA), and Asian Institute of Technology (AIT).

Saunders et al. (2003) argue that questionnaires seldom result in a full response and a return rate is low. Nevertheless, good questionnaires lead to clear and unconfused replies (Birley & Moreland, 1998). Thus, in order to create an effective questionnaire which is relevant to the topic, the researcher has applied literature from secondary data such as books, academic journals and website.

3.2 Design of Questionnaire

Part 1: General background

Question 1 to 8 used to getting general background and experience in order to group the idea what overall questionnaire gone to be about.

Part 2: What important factors that your organization operates.

Question 9-34 used performance ratings since the researcher is interested in measuring idea of how respondents think about business continuity each determinants which using a five-point Likert-Scale to study the factors opinion of business continuity management.

3.3 Sampling and Procedure

Sampling technique provide a variety of methods that help the researcher to reduce the amount of data and lead to specific data. Saunders et al.(2003) also say that sampling provides an alternative to a census because it would be impracticable to survey the whole population and the budget and time will be too limited to survey the entire population. Therefore, in this research will cover only 400 MBA or Ph.D. students.

Target population

Target population of this research will be both male and female, MBA or higher educated to understand business management term, aged between 20 year old to more than 65 year old people, who have work experience. Respondents came from Stamford International University (STIU), Ramkhamhaeng University, National Institute of Development Administration (NIDA), and Asian Institute of Technology (AIT). These respondents understand the concept of business continuity also work experience will help their answer the questionnaire.

Sample size

Sample size means the number of observations or cases specified by the estimated variance of the population, the estimated proportion is used to specify the sample size without knowing the number of population. To determine sample size for a proportion, the researcher uses a desired level of confidence 95% and the maximum allowance for random sampling error is 5%, which is the magnitude of acceptable error, or the confidence level (Zikmund, 1994). The theoretical of Levine, Berenson, & Stephan (1999) is applied in this research. The formula below is used to calculate the require sample size for problems involving proportions:

$$n = \frac{Z^2 p(1-P)}{e^2}$$

where: *n* = number of sample size

Z= Z score based on researcher's desired level of confidence, which is 95% therefore, z=1.96

P= the true proportion of "success". It is actually the population parameter. As the past information and relevant experience is not available, the researcher determine the value that will make p(1-p) as large as possible. Levine, Berenson, & Stephan (1999) stated that the true proportion p=0.5 id consider as the most conservative way of determining the sample size

E= an acceptable sample error, which is estimated at 5%

$$N = \frac{Z^2 p(1-P)}{e^2} = \frac{(1.96)^2(0.5)(1-0.5)}{(0.05)^2}$$

$$= 384$$

From the calculation, the minimum number of sample is 384, is required in this research. Therefore, respondent will be 400 MBA or Ph.D. students were distributed as the researcher expected to earn more reliable result in the collection of primary data.

3.4 Data Analysis

Saunders et al. (2003) state that research will involve some numerical data or contain data that could be quantified to answer the research question and meet the dissertation objectives so that the data need to be analysed and interpreted.

As this research is base on quantitative data, Statistical Package for the Social Sciences (SPSS) programme was used for analysis. The research finding and analysis will consist of Descriptive Statistics which includes counts (numbers or frequencies) ;

proportions (percentages), All of the analysis methods are analyzed by SPSS Verison 17.

As some of the statiscal applied in the chapter 4 was related to an advanced statistical analysis technique, this part aims to explain and evalutate the use of the data analysis methods which the author adopts in analysis part. The theories in statistical subject have also been discussed.

Descriptive Statistic Analysis

According to Zikmund (2003), in descriptive statistics, the calculation of the average, frequency distribution, and percentage distribution are the most common forms of summarizing data. This tool transform the raw data into a form that will make it easy for researchers to interpret and understand their findings.

Correlation

Correlation is use to study the relationship between two or more variables. Correlation coefficient will use the symbol represents the correlation coefficient of the group and represents the correlation coefficient of the population Correlation coefficient to measure. Size of the relationshipbetweenthetwovariablesis-1 ≤ r ≤ 1and0 ≤ r ≤ 1.

Levels or the size of the relationship that use to correlation coefficient. If the correlation coefficient is close to -1 or 1 indicates a high degree of correlation. If it is very close to 0 indicate a relationship with little or no for. Considering the correlation coefficients generally may use the following criteria (Hinkle, 1998)

R	The level of the relationship
0.90 to 1.00	Very high
0.70 to 0.90	High
0.50 to 0.70	Moderate
0.30 to 0.50	Low
0.00 to 0.30	Very low

ANOVA (analysis of variance)

ANOVA is a technique to determine if statistically significant differences in means occur between two or more groups. This technique is referred to as "one-way" because there is only one independent variable (even though there may be several levels of that variable). The *F*-test is a procedure for comparing one sample variance to another sample variance and determines whether there is more variability in the scores of one sample than in the scores of another sample. The *F*-distribution measures whether the variability of two samples differs significantly; if the statistic is greater than the *t*-value for some level of significance, there is no significant difference in the means of the sample and the hypothesis may be rejected (Zikmund, 2003).

Formula of calculation of *F*-Ratio

$$F = \frac{\text{MS Between}}{\text{MS Within}}$$

MS = Mean Square

Pearson product-moment correlation coefficient

Pearson correlation coefficient, the symbol rxy is a measure of the relationship. Between two variables or data sets at two variables or data sets will be in the form of data. Section interval or ratio (Interval or Ratio scale) as the correlation between the conditions Health and viewing.

$$r_{xy} = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{\left[N\sum X^2 - (\sum X)^2\right]\left[N\sum Y^2 - (\sum Y)^2\right]}}$$

3.5 Data Measurement

Table 3.1 Part I Operationalization of the Independent Variables

Independent Variables	Concept Definition	Operational Components	Scale of Measurement	Question No.
Gender	*The sexuality of respondent in this study*	□ Male □ Female	Nominal	Q.1
Age	*The age of respondent in this study*	□ 20-25years old □ 26-30 years old □ 31-35 years old □ 36-40 years old □ More than 40 years old	Nominal	Q.2
Educational Level	*The education background of the respondent*	□ Master Degree □ PH.D. or Higher	Nominal	Q.3
Occupation	*What kind of job therespondent doing*	□ CEO □ CFO □ MD □ GM □ Director □ Manager □ Assistant Manager □ Supervisor □ Other_____	Nominal	Q.4

Table 3.1 Part I Operationalization of the Independent Variables (Cont.)

Independent Variables	Concept Definition	Operational Components	Scale of Measurement	Question No.
Has your company been affected by, or at risk for, any of the following business interruptions (Fill in all that apply):	*What experience therespondent been*	□ Natural Disaster □ Hardware Failure □ Software Failure □ Human Error □ Power Outage □ Service Provider Failure □ Other_____	Nominal	Q.5
How seriously is crisis business interrupts taken at your organization?	*What kind of business interruptstake place for respondent*	□ Not at all □ Low □ Moderately □ Very □ Extremely	Nominal	Q.6
How frequently your organization faces the interruption per year?	*How offen their face the interruption per month*	□ 0-1 times □ More than 1-3 times □ More than 3-5 times □ More than 5 times	Nominal	Q.7

Table 3.1 Part I Operationalization of the Independent Variables (Cont.)

Independent Variables	Concept Definition	Operational Components	Scale of Measurement	Question No.
What is the expected recovery time for your critical business functions?	*What their expectation for recovery time for critical business functions*	□ 0-4 hours □ 4-8 hours □ Within one day □ 1-2 days □ More than 2 days □ NA □ Other_____	Nominal	Q.8

Table 3.2 Part II Operationalization of the Independent Variable

Independent Variables	Concept Definition	Operational Components	Scale of Measurement	Question No.
Business Continuity Plan	*Perception about how their organization perform*	□ Totally Agree □ Agree □ Fairly □ Disagree □ Totally Disagree	Interval	Q.9-13
Business Impact Analysis	*How respondent perception their organizationidentify business impact.*	□ Totally Agree □ Agree □ Fairly □ Disagree □ Totally Disagree	Interval	Q.14-18

Table 3.2 Part II Operationalization of the Independent Variable (Cont.)

Independent Variables	Concept Definition	Operational Components	Scale of Measurement	Question No.
Risk Analysis	*How their organization control the risk analysis*	□ Totally Agree □ Agree □ Fairly □ Disagree □ Totally Disagree	Interval	Q.19-23
IT Recovery Plan	*Respondent perception about how their organization plan for IT*	□ Totally Agree □ Agree □ Fairly □ Disagree □ Totally Disagree	Interval	Q.24-28
Testing and Revising	*How their organization perform test and revising of their plan*	□ Totally Agree □ Agree □ Fairly □ Disagree □ Totally Disagree	Interval	Q.29-33

Table 3.3 Part II Operational organization of the Dependent

Dependent Variable	Conceptual Definition	Operational Components	Level of Measurement	Question No.
Business Continuity Management	*The respondent judgment about the overall preparedness for disaster*	□ Totally Agree □ Agree □ Fairly □ Disagree □ Totally Disagree	Interval	Q.34

CHAPTER 4

RESEARCH FINDINGS

In this chapter will discuss about the evaluations of survey and analyzes the results of all the collected data. This data was distributed to 400 respondents in focus area. The analysis includes 4 parts which is concluded explaining of the demographics of the samples and their evaluations, analyze the results of the hypothesis testing.

4.1 Descriptive Analysis

Descriptive statistics are used to describe the basic features of the data and summary the sample and measures. Together with simple graphics analysis, statistics form the basis of virtually every quantitative data analysis.

Frequency Distribution

The first part of the Questionnaire, the respondents more than half are female with total number 212 or 53% and the rest are male respondents of 188 (47%) making females the majority of the respondents of this questionnaire. Age of respondents shows the major group of respondents' ranges from 26-35 years old, a total of 293 respondents (73.3%). Respondents more than 40 years old, totaling 4 persons (1%), those between 36-40 years old, 53 respondents (13.3%), those 18-25 years old added to 50 respondents (12.5%).The education of respondents illustrates the education level of respondents. This table shows that the total number of respondents is currently a master degree 400 (100%). Job tittle\Division of Respondents show the frequency of the 400 samples selected for the research. As the Table shows, in the research period, there are Manager 98 (24.5%). 96 respondents are Assistant Manager or 24%. 78 respondents are Supervisor (19.5%), 63 Director (15.8%), 21 respondents are other job (5%), 15 respondents (3.8%) were MD. CFO and GM are same 13 or 3.3%. The rest of the respondents were CEO 3 or 08%.

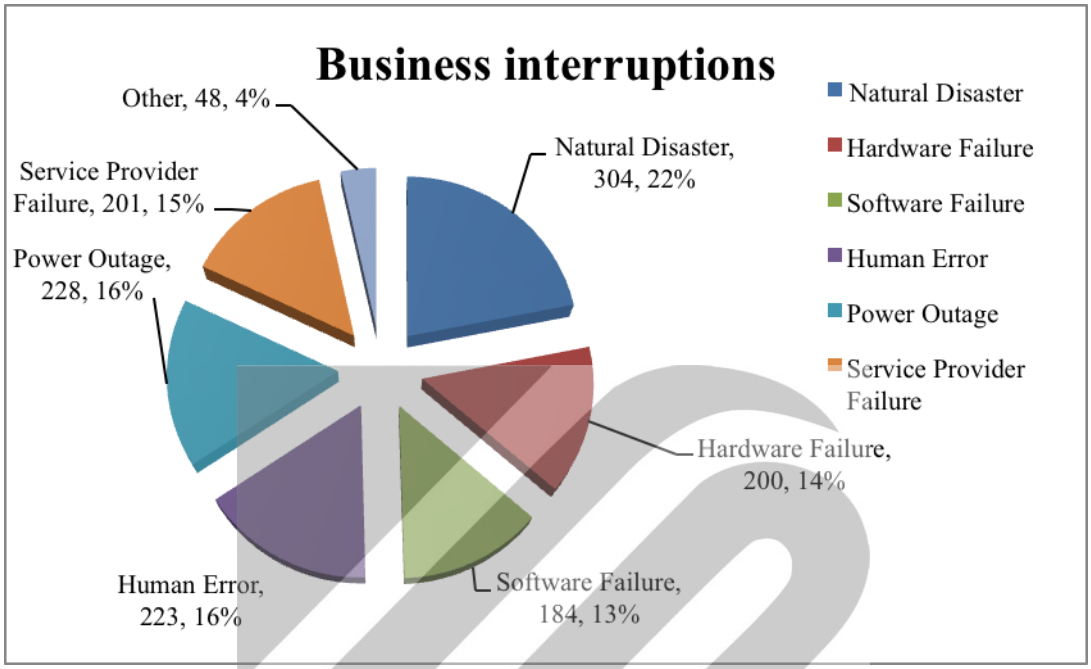

Figure 4.1 Frequency Distribution- Business Interruptions

Figure 4.1 showed that the type of disaster of respondents had face in business, for a largest number of respond is Natural Disaster with a total of 304 persons (22%) This answer was the largest because most people affect from flooding at 2011 directly or indirectly way. Moreover respondent of 228 or (16%) answer that they faced Power Outage that able to happen from many factor to conclude that is un-predictable. For 223 respondents (16%) affected by Human Error this may occur from their knowledge to do their job role1 or mistake, and 200 respondents (14%) were hardware Failure which normal happen when hardware getting old and Service Provider Failure at 201(15%) such as internet down, cabling problem that uncontrol. The rest of 184 respondents (13%) were Software Failure.

Figure 4.2 Frequency Distribution- crisis of business interrupts

Figure 4.2 showed their business attend in business interruption. Some of respondents selected "extremely" 100 persons (25%) this mean it's important for business such as running of telecommunication, service provider, or manufacturing, government service that would be zero downtime. However, large firm are able to relocate their employee to somewhere else for emergency office. 223 respondents (55.8%) is selected "very" such reseller, IT business, hotel that accept some downtime following the policy and steps. and another 71 respondents selected "moderately" (17.8%) such Small and Medium Enterprise which do not have risk and management control. 6 of respondents (1.5%) selected "low" is not relate with IT system much.

Figure 4.3 shows the often of organization has interrupt their business that their organization thought, most respondent answered"0-1 time" with number of 310 respondents (77.5%) less interruption means business running more stable and receive more reputation. However, 78 respondents (19.5%) faced more than 1-3 times of organization interrupt that acceptable for some people. However, the external factor is uncontrollable that make organization often face the interruption this depend on many factors such as location, policy, and management. Moreover, the 12 persons (3%)

faced interruption more than 3-5 times per year that quite unacceptable for large organization.

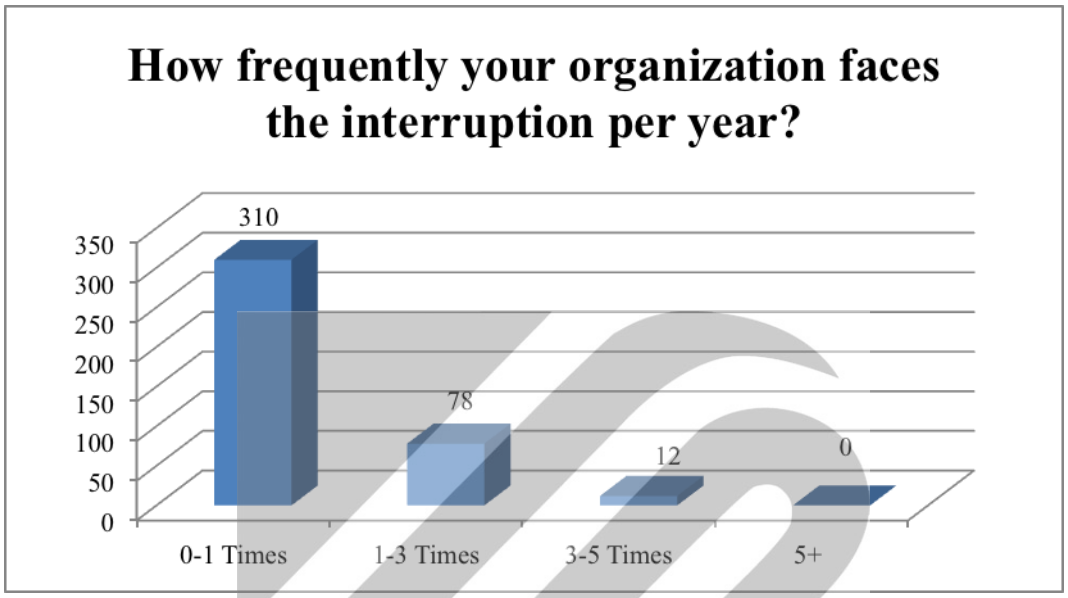

Figure 4.3 Frequency Distribution – the frequently of interruption per year

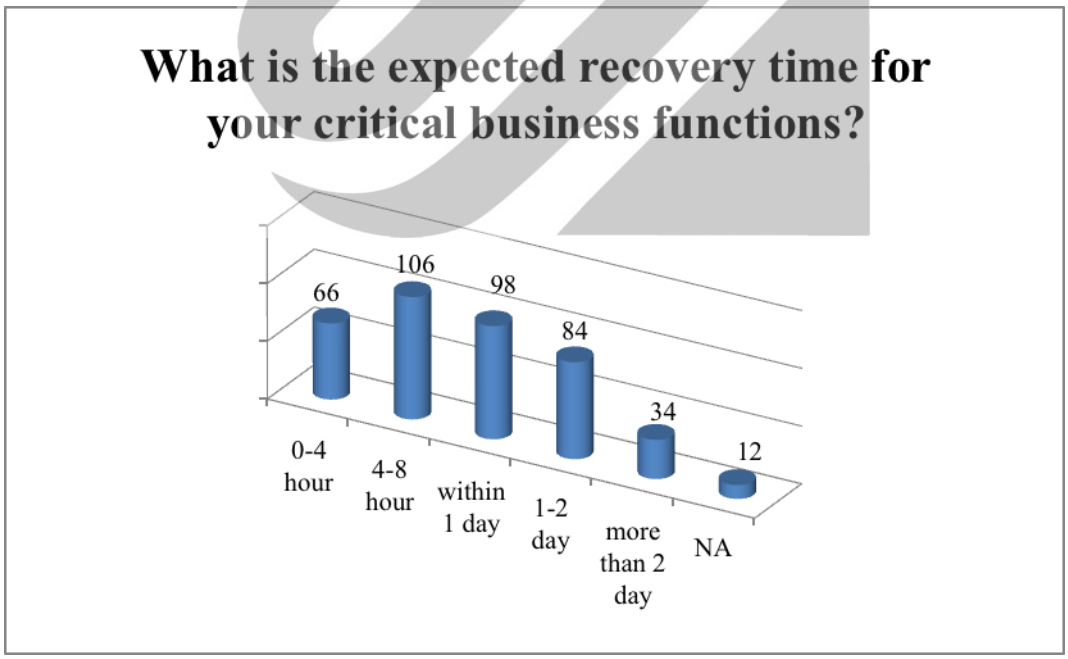

Figure 4.4 Frequency Distribution – the expected recovery time

Figure 4.4 showed the expect time of recovery time of 66 respondents (16.5%), it should be with in 0-4 hours it's mean make it fast as possible to continuity. The

large respondent expected 4-8 hours or 106 respondents (26.5%) that acceptable for 4-8 hour of time. On the other hand 98 or 24.5% expected within 1 day should be able get it back. 84(21%) respondents expected 1-2 day when external factor involved. To sum up, the recovery time most of people want as fast as the organization able to do it but it depend on the process of the recovery some event able to recovery faster than the another such as Sale department was unable to connect the stock and accounting unable to access database on the other hand the human resource lost a file. The recovery time of sale department and accounting functions may take longer time that just recover file for human resource.

Summary of the first part of the questionnaire is male and female in Master education and may kind in work filed think that business can be interrupt in many way however it deepens on the policy to prepare for disaster. Most of respondent take the interruption serious but on anther hand their organization face less interruption per year. However, the exception for recovery time is varies the faster mean better for recover time

4.2 Variable Mean and Standard Deviation

As the **Table *Reliability Analysis-Scale (Alpha) of Pretest Result*** shows that the outcome of the reliability analysis-scale or obtained alpha of .827 items was 26. Which is greater than 0.6. Therefore, it could be make sure that this research's questionnaire was reliable. The Table shows the reliability analysis-scale of the pretest result.

Reliability Statistics

Table 4.1 Reliability Statistics

Cronbach's Alpha	N of Items
.827	26

Table 4.2 Variable Mean and Standard Deviation-Business Continuity Plan

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Organization should prepare for disaster	400	2	5	4.23	.729
Organization should have more than one business continuity plan	400	2	5	4.21	.741
Documented crisis planning management process has to be within organization policy	400	1	5	4.18	.807
Organization should have a dedicated team of professionals focused on business continuity	400	2	5	4.19	.744
A good Business Continuity plan can help the organization to restart faster	400	2	5	3.81	.745
Valid N (listwise)	400				

Table 4.2 showed the Business Continuity Plan of organization should prepare for disaster high level of influence with Mean = 4.23. Also, Organization should have more than one business continuity plan high level of influence with Mean =4.21 and Organization should have a dedicated team of professionals focused on business continuity Mean= 4.19. Moreover, documented crisis planning management process has to be within organization policy with Mean = 4.18.The rest are high level of influence Mean =3.81.

Table 4.3 Variable Mean and Standard Deviation-Business Impact Analysis

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
The business impact analysis phase would involve the identification of the functions most critical to ensure business continuity	400	2	5	4.30	.739
The better Business Continuity plan be created, the loss less money	400	2	5	4.14	.794
The customers will continue with the same company when the company shows a good business continuity plan when the disaster occur (reputation)	400	2	5	4.26	.694
The better Business Continuity plan, the better management control	400	2	5	4.25	.712
How much organization identified important core of business, the fast organization restart	400	2	5	4.24	.733
Valid N (listwise)	400				

Table 4.3 showed the analysis of Business Impact Analysis that effect on business that would involve the identification of the functions most critical to ensure

business continuity highest level of influence with Mean = 4.30. Also, the customers will continue with the same company when the company shows a good business continuity plan when the disaster occur (reputation) highest level of influence with Mean =4.26. The better Business Continuity plan, the better management control Mean= 4.25. Moreover, How much organization identified important core of business, the fast organization restart influence with Mean = 4.24. The rest the better Business Continuity plan be created, the loss less money
Influence Mean =4.14.

Table 4.4 Variable Mean and Standard Deviation-Business Continuity - Risk Analysis

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Risk analysis is the identification of procedures that could possibly prevent or reduce the effect of a disaster	400	2	5	4.15	.794
Organization should prepare for the risk by educating their employee	400	2	5	4.40	.742
The better Business Continuity plan be created, the well of treat and control risk occur	400	2	5	4.22	.735

Table 4.4 Variable Mean and Standard Deviation-Business Continuity - Risk Analysis (Cont.)

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
The better Risk Analysis plan, the better management of share and transfer risk to other organizations (insurance)	400	2	5	4.14	.753
How much organization identified risk, the opportunity business can take	400	2	5	4.19	.749
Valid N (listwise)	400				

Table 4.4 showed the analysis of the Risk Analysis that Organization should prepare for the risk by educating their employee with highest Mean =4.40.The better Business Continuity plan be created, the well of treat and control risk occur with Mean =4.22. How much organization identified risk, the opportunity business can take Mean =4.19.Risk analysis is the identification of procedures that could possibly prevent or reduce the effect of a disaster with Mean =4.15. The better Risk Analysis plan, the better management of share and transfer risk to other organizations (insurance) influence Mean =4.14.

Table 4.5 Variable Mean and Standard Deviation-IT Recovery Plan

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
The IT system should be available at first priority to continuity the business	400	2	5	4.20	.782
Data recovery has to be chosen as a first step towards a recovery plan	400	2	5	4.17	.806
Offside backup is require for business continuity plan	400	2	5	4.20	.751
Financial performance and SME budgetary issues are bound to play a role when it comes to choosing an appropriate backup strategy	400	2	5	4.32	.748
The recovery of IT systems and applications needed by the various business functions	400	2	5	4.41	.677
Valid N (listwise)	400				

Table 4.5 showed the analysis of the IT Recovery Plan that the recovery of IT systems and applications needed by the various business functions with highest Mean =4.41.Financial performance and SME budgetary issues are bound to play a role when it comes to choosing an appropriate backup strategy with Mean =4.32 Offside backup is require for business continuity planned the IT system should be available at first

priority to continuity the business got the same Mean = 4.20. The last is Data recovery has to be chosen as a first step towards a recovery plan with Mean=4.17

Table 4.6 Variable Mean and Standard Deviation-Testing and Revising

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Business Continuity plan or Disaster Recovery should test at least one time a year	400	1	5	4.26	.718
Test and revising of contingency plan make the plan up-to-date	400	2	5	4.15	.775
Testing programs help employees know where to go for information and what to expect in a crisis	400	1	5	4.21	.780
Every employee should involve Business Continuity plan or Disaster Recovery testing	400	1	5	4.20	.759
Test and revising help organization identify flaws in the plan	400	2	5	4.17	.741
Valid N (listwise)	400				

Table 4.6 showed the analysis of the Testing and Revising that testing programs help employees know where to go for information and what to expect in a crisis with highest Mean =4.26.Testing programs help employees know where to go for information and what to expect in a crisis with Mean =4.21 Every employee

should involve Business Continuity plan or Disaster Recovery testing with Mean = 4.20. Test and revising help organization identify flaws in the plan with Mean =4.17.The last is Test and revising of contingency plan make the plan up-to-date with Mean=4.15.

Table 4.7 Variable Mean and Standard Deviation- Business Continuity Management

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
The Business Continuity Management is important for organization	400	3	5	4.25	.681
Valid N (listwise)	400				

Table 4.7 showed the analysis of the Business Continuity Management is important for organization that influence with Mean = 4.25

4.3 Regression Analysis

Table 4.8 Regression Analysis- Business Continuity Plan

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.923[a]	.852	.850	.284

a. Predictors: (Constant), BCP13, BCP12, BCP10, BCP11, BCP9

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	181.804	5	36.361	452.305	.000[a]
	Residual	31.674	394	.080		
	Total	213.477	399			

a. Predictors: (Constant), BCP13, BCP12, BCP10, BCP11, BCP9

b. Dependent Variable: important

Table 4.8 Regression Analysis- Business Continuity Plan (Cont.)

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.355	.143		2.487	.013
	BCP9	.940	.039	.936	24.158	.000
	BCP10	-.016	.038	-.016	-.407	.684
	BCP11	-.002	.018	-.002	-.087	.931
	BCP12	-.019	.019	-.019	-.973	.331
	BCP13	.015	.019	.015	.786	.433

a. Dependent Variable: important

ANOVA, Sig =0.000 <0.05, then accept H_1 therefore it can be conclude Business Continuity Plan correlate with business continuity management

Model Summary, the result of R Square = .852 = 85.2% means that Business Continuity Plan have a positive direct effect on Business Continuity Management by 85.2%.

Coefficients, showed that question 9 and 13 are positive relationship and other are negative relationship

$H1_0$ Business Continuity Plan will have no positive direct effect on Business Continuity Management.

$H1_1$ Business Continuity Plan will have a positive direct effect on Business Continuity Management.

Table 4.9 Regression Analysis- Business Impact Analysis

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.802[a]	.643	.638	.440

a. Predictors: (Constant), BIA18, BIA15, BIA14, BIA17, BIA16

Table 4.9 Regression Analysis- Business Impact Analysis (Cont.)

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	137.220	5	27.444	141.795	.000[a]
	Residual	76.258	394	.194		
	Total	213.477	399			

a. Predictors: (Constant), BIA18, BIA15, BIA14, BIA17, BIA16

b. Dependent Variable: important

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.374	.215		1.741	.082
	BIA14	.025	.030	.025	.827	.409
	BIA15	.009	.028	.010	.336	.737
	BIA16	.336	.066	.318	5.122	.000
	BIA17	.263	.057	.256	4.635	.000
	BIA18	.277	.060	.278	4.629	.000

a. Dependent Variable: important

ANOVA, Sig =0.000 <0.05, then accept H_1 therefore it can be conclude Business Impact Analysis will have a positive direct effect on Business Continuity Management..

Model Summary, the result of R Square = .643 = 64.3% means that Business Impact Analysis will have a positive direct effect on Business Continuity Management by 85.2%.

Coefficients, showed that all variable positive relationship

$H2_0$ Business Impact Analysis will have no positive direct effect on Business Continuity Management.

H2₁ Business Impact Analysis will have a positive direct effect on Business Continuity Management.

Table 4.10 Regression Analysis- Risk Analysis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.710[a]	.504	.497	.519

a. Predictors: (Constant), Risk23, Risk22, Risk19, Risk20, Risk21

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	107.549	5	21.510	80.005	.000[a]
	Residual	105.929	394	.269		
	Total	213.477	399			

a. Predictors: (Constant), Risk23, Risk22, Risk19, Risk20, Risk21

b. Dependent Variable: important

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.893	.274		3.255	.001
	Risk19	.037	.033	.040	1.116	.265
	Risk20	.112	.036	.114	3.082	.002
	Risk21	.679	.037	.682	18.227	.000
	Risk22	-.030	.036	-.031	-.819	.413
	Risk23	-.009	.035	-.009	-.248	.804

a. Dependent Variable: important

ANOVA, Sig =0.000 <0.05, then accept H_1 therefore it can be conclude Risk Analysis will have a positive direct effect on Business Continuity Management.

Model Summary, the result of R Square = .504 = 50.4% means that Risk Analysis will have a positive direct effect on Business Continuity Management by 50.4%.

Coefficients, showed that question number 19, 20, and 21 are positive relationship and other are negative relationship

$H3_0$ Risk Analysis will have no positive direct effect on Business Continuity Management.

$H3_1$ Risk Analysis will have a positive direct effect on Business Continuity Management.

Table 4.11 Regression Analysis- IT Recovery Plan

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.159[a]	.025	.013	.727

a. Predictors: (Constant), IT28, IT27, IT24, IT26, IT25

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.388	5	1.078	2.040	.072[a]
	Residual	208.089	394	.528		
	Total	213.477	399			

a. Predictors: (Constant), IT28, IT27, IT24, IT26, IT25

b. Dependent Variable: important

Table 4.11 Regression Analysis- IT Recovery Plan (Cont)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.457	.374		9.240	.000
	IT24	.069	.048	.074	1.429	.154
	IT25	.104	.048	.114	2.177	.030
	IT26	.023	.051	.023	.442	.659
	IT27	.018	.051	.019	.357	.721
	IT28	-.025	.055	-.023	-.454	.650

a. Dependent Variable: important

ANOVA, Sig =0.000 <0.05, then reject H_1 therefore it can be conclude IT Recovery Plan will have no positive direct effect on Business Continuity Management

Model Summary, the result of R Square = .025 = 2.5% means IT Recovery Plan will have no positive direct effect on Business Continuity Management by 2.5%.

Coefficients, showed that question 24, 25, 26, and 27 are positive relationship and another are negative relationship

$H4_0$ IT Recovery Plan will have no positive direct effect on Business Continuity Management.

$H4_1$ IT Recovery Plan will have a positive direct effect on Business Continuity Management.

Table 4.12 Regression Analysis- Testing and revising

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.195[a]	.038	.026	.722

a. Predictors: (Constant), Test33, Test29, Test31, Test30, Test32

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.143	5	1.629	3.125	.009[a]
	Residual	205.334	394	.521		
	Total	213.477	399			

a. Predictors: (Constant), Test33, Test29, Test31, Test30, Test32

b. Dependent Variable: important

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.176	.332		9.573	.000
	Test29	.079	.053	.078	1.488	.138
	Test30	-.020	.051	-.022	-.401	.689
	Test31	.146	.050	.156	2.923	.004
	Test32	-.024	.052	-.025	-.466	.641
	Test33	.072	.052	.073	1.390	.165

a. Dependent Variable: important

ANOVA, Sig =0.000 <0.05, then accept H_1 therefore it can be conclude Testing and revising will have a positive direct effect on Business Continuity Management.

Model Summary, the result of R Square = .038 = 3.8% means that Testing and revising will have a positive direct effect on Business Continuity Management.t by 3.8%.

Coefficients, showed that question 29, 31, and 33 are positive relationship and another are negative relationship

$H5_0$ Testing and revising will have no positive direct effect on Business Continuity Management.

$H5_1$ Testing and revising will have a positive direct effect on Business Continuity Management.

CHAPTER 5

SUMMARY, CONCLUSION AND RECOMMENDATIONS

In this chapter consists of 4 sections. The first section is interpretation of the results or conclusions. Section two includes discussion which is used to answer the statement of problem and achieve the objectives. Additional the results from the study will generate the idea to recommend and suggest for the section three. The last section is the further study area.

5.1 Conclusions

This reaserch aims to examine the variable that has relationship for Business Continuity Management and to examine the differences between Business Continuity Management and its determinants. The evaluations are based on the comparison of the demographics of the including gender, age, education, job tittle/division, company affected, crisis business interrupts, frequently of interruption' per year, the expected recovery time, and Business continuity management.

Table 5.1 The summary of the findings

Demographic	Highest Proportion	Percentage
Gender	Female	53%
Age	26-35 years old	73.3%
Education Level	Master Degree	100%
Job tittle\Division	Manager	24.5%
Company affected	Natural Disaster	22%
Crisis Business interrupts	Very	55.8%

Table 5.1 The summary of the findings (Cont.)

Demographic	Highest Proportion	Percentage
Frequently of interruption per year	0-1	77.5%
The expected recovery time	4-8	26.5%

The Results of Hypothesis Testing with Regression Analysis

Table 5.2 The summary of the Hypothesis testing

	Hypothesis
H1	$H1_1$: Business Continuity Plan will have a positive direct effect on Business Continuity Management.
H2	$H2_1$: Business Impact Analysis will have a positive direct effect on Business Continuity Management.
H3	$H3_1$: Risk Analysis will have a positive direct effect on Business Continuity Management.
H4	$H4_0$: IT Recovery Plan will have no positive direct effect on Business Continuity Management.
H5	$H5_1$: Testing and revising will have a positive direct effect on Business Continuity Management.

5.2 Discussion

Business Continuity Management is most important, as business grow up related to the study that nowadays there are plenty of book, case study, methodology, standard, and research on business continuity management. Therefore, many

organizations focus more on risk analysis and control then setup the policy and train their staff more often to avoid the risk such as fire training as a standard twice a year. Testing power outage and start up power generator every one or two month for standby when the interruption comes.

Other the other hand, organizations seems to have business continuity management to prepare or avoid the risk, but some have not managed policies or measures. Organizations do not design properly what to do when a problem occurs or nearly to happen, most of them are small and medium size organization. However, for large organization they have got the specialist team to mange or prepare this such as risk and management control.

The study and questionnaire is able to answer and understand on the research question that the effectiveness of business continuity management can bring back business faster. After hypothesis testing Business Continuity Plan, Business Impact Analysis, Risk Analysis, and Testing and revising have positive direct effect on Business Continuity Management. However, IT Recovery Plan has no positive direct effect on Business Continuity Management.

According to the 5 hypotheses that show the relationship between various factors that includes Business Continuity Plan, Business Impact Analysis, Risk Analysis, IT Recovery Plan, and Test and Revising. The regression analysis shows the study of Business Management Continuity Management have relationships with Business Continuity Plan, Business Impact Analysis, Risk Analysis, and Testing and revising.

5.3 Recommendation

The study show that business able to face the interruption in many ways, but the business can be able to set up the plan and policy to minimal the damage and fast respond for an event. After all, the conceptual model of Business Continuity Management in this study will help the business to focus the lists what would be include for preparing a plan. Also, the IT system play as important role if a business face with interruption from any disaster or crisis at anytime, it will effect internal and external organization. Therefore, the best of business continuity management will help

organization survive. “Any organization will take it serious to prepare for business continuity when they already suffer from it.”

5.4 Further Studies

- **Other factors**

This research only focuses only business continuity management and its determinants. For further study, there are more concerning variable that should be including on document protection, communication crisis management.

- **Other Areas**

The scope of this research is respondents only 400 MBA or Ph.D. students from Stamford International University (STIU), Ramkhamhaeng University (RU), National Institute of Development Administration (NIDA) , and Asian Institute of Technology (AIT). The data are collected from target population from those areas. Further research should extend to other business location and regions such as northern part, north-eastern part, southern part or eastern part of Thailand, and other disasters

- **Deeper in Demographic Characteristics**

Other consideration, future studies could also look deeper into the study of effect of the differences of demographic characteristic factors toward Business Continuity Management.

REFERENCES

Aon Corporation. (2011). *Thailand Floods Event Recap Report.* Retrieved 2013, from http://thoughtleadership.aonbenfield.com/Documents/20120314_impact_forecasting_thailand_flood_event_recap.pdf

Arregoces, M., & Portolani, M. (2003). *Data Center Fundamentals.* Cisco System.

Button, D. E. (1995). *Dynamic Business Continuity Planning.* port Elizabeth Technikon, Port Elizabeth, South Africa: Unpublished master's thesis.

Bell, J. (1999). *DOING YOUR RESEARCH PROJECT* (3rd ed.). Buckingham: Open University.

Birley, G., & Moreland, N. (1998). *A Practical Guide to Academic Research.* London.

Boddington, T. (1998). *Preparing for BS 7799 certification: Guidance on implementation requirements to organisations preparing for certification.* London: British Standards Institution.

Centre of Research on Epidemiology of Disaster– CRED. (2012). *EM-DAT: The OFDA/CRED International Disaster Database.* Retrieved 2013, from http://www.emdat.be/result-disaster-profiles?disgroup=natural&dis_type=Flood&period=1900$2012

Colraine. (2005). *Preparedness for emergency response.*

Devargas, M. (1999). Survival is Not Compulsory: An Introduction to Business Continuity Planning. p 35-46.

DisasterRecovery.org. (2012). *Business Continuity & Disaster Recovery Planning.* Retrieved 2013, from http://www.disasterrecovery.org/disaster_recovery.html

F5 Networks Inc. (2012). *New technology for disaster recovery/ Business Continuity*. Retrieved 2013, from https://www.f5.com/pdf/solution-guides/disaster-recovery-guide1.pdf

Florendo, R., Martens, J., Middlebrooks, R., Romanyschyn, J., & Solter, M. (1998). *Internet Disaster Recovery Concepts* . nited States of America: International Business Machines Corporation .

Gulley, T. (1999). Is Your Data Safe? . *Protecting Critical Data in a Distributed Computing Environment* .

REFERENCES (Cont.)

Guttman, & Roback. (1995). *An introduction to computer security.* The National Institute of Standards and Technology (NIST).

Glenn, J. (2002). What Is Business Continuity Planning? How Does It Differ From Disaster Recovery Planning? Disaster Recovery Journal.

Goggins, K. (1999). *Contingency Planning 101*. Contingency Planning & Management.

Gordon, C. (2000). How to Cost Justify a Business Continuation Plan to Management. *Disaster Recovery Journal* .

Gregory, P. H. (2007). *IT Disaster Recovery Planning For DUMMIES.*

Hassim, M. (2000). *To plan or not to plan?* Accountancy SA .

Hawkins, S. M., Yen, D. C., & Chou, D. C. (2000). Disaster recovery planning: a strategy for data security. *8* (5), p. 222-229.

Heng, G. M. (1996). Developing a suitable business continuity planning methodology. *4* (2), p. 11-13.

Hinkle, D. (1998). Applied Statistics for the Behavioral Sciences. p. 118.

Hurwicz, M. (2000). When Disaster Strikes (Industry Trend or Event).

Hyde. (2000). Recognizing deductive processes in qualitative research. *40* (11/12), p. 1194-1209.

IBM Global Services. (1999). *Business Continuity: New risks, new imperatives and a new approach*. Retrieved 2013, from http://www-07.ibm.com/services/pdf/buscont.pdf

IBM Global Services. (2000). *Managing information technology in a new age*. Retrieved 2013, from http://www-935.ibm.com/services/us/its/pdf/g510-1178-00.pdf

Ismail, S. A. (2005). *The evaluation on Disaster recovery plan and Data Recovery in Pusat Sistem Maklumat Bersepadu (PSMB), Universiti Teknologi Mara (UiTM).* Universiti Teknologi MARA.

Kearvell-White, B. (1996). *National (UK) Coputer Security Survey.* Magazine Computer Security.

REFERENCES (Cont.)

King, J. W. (2000). *Business Continuity Planning & the highly protected risk expanding the envelope: Planning for the entire organisation.* Disaster Recovery Journal.

Koski, K. (2001). *Backup and Offsite Vaulting.*

Lapedis, R. (2001). *Disaster Recovery: No Longer Enough.* Disaster Recovery Journal.

Larue, J. (2000). *How Far is Really Far Enough Away?* Disaster Recovery Journal.

Levine, D., Berenson, M., & Stephan, D. (1999). *Statistics for managers.*

Levine, R. (2009). *Recovery point objective - recovery time objective strategy.*

Lumpp, T., Schneider, J., Holtz, J., Mueller, M., Lenz, N., Biazetti, A., et al. (2008). From High Availability and Disaster Recovery to Business Continuity Solutions. *47* (4), p. 605-619.

Malhotra, N. K., & Birks, D. F. (2005). *Marketing Research: An Applied Approach.*

McKinney, C. C. (2000). *Does your plan measure up? Contingency Planning & Management.*

Morwood, G. (1998). Business continuity: awareness and training programmes. *6* (1), p. 28-32.

Paradine. (1995). *Business interruption insurance : a vital ingredient in your disaster recovery plan.*

Peterson, C. A. (2009). *Business Continuity Management & Guidelines.*

Ranjan, P., Kumar, P., & Abhishek, K. (2012). Business Continuity Planning in Indian Perspective. *Journal of Advances in Computational Research: An International Journal* .

Reuvid, J. (2006). *Managing business risk: A practical guide to protecting your business* (2nd ed.).

Robbins-Gioia. (2003). *Implementing and Maintaining Project Management* (Vol. 2).

Roberson, J. (2000). *Personal Communication.*

Saunders, M., Lewis, P., & Thornhill, A. (2003). *Research Methods for business students* (3rd ed.). England, Essex: Pearson.

REFERENCES (Cont.)

Savage, M. (2002). Business continuity planning. *51* (5), p. 254-261.

Scheur Management Group. (1999). *How Healthy Is Your Business.*

Smith, M., & Sherwood, J. (1995). Business Continuity Planning. Computers & Security. *14* (1), p. 14-23.

Tydlaska, L. (1996). *What's Behind Your backup Plan. Contingency Planning & Management.*

Toigo, J. W. (2003). Disaster Recovery Planning: Preparing for the Unthinkable . (3rd Ed.)

Underwood, M. (1998). Disaster recovery services help keep operations flowing for AS/400 systems.

Wilson. (2000). Business Continuity Planning: A Necessity In The New E- Commerce Era.

Zikmund. (2003). *Exploring marketing research* (9th ed.). Thomson-South Western.

APPENDIX A

QUESTIONNAIRE

STAMFORD INTERNATIONAL UNIVERSITY RESEARCH PROJECT QUESTIONNAIRE

This questionnaire consists of three sections, 34 items are included.
Please answer all of the questions. There is no right or wrong answer.
Your spontaneous and honest response is important to the success of this research.

Part1: General Background (item 1-4): *For each question, please put "√" on one answer which is most applicable to you.*

1. Gender: □ Male □ Female

2. Age:

□ 20-25years old □ 26-30 years old

□ 31-35 years old □ 36-40 years old □ More than 40 years old

3. Educational level:

□ Master Degree □ Ph.D. or higher

4. Job Tittle/Division:

□ CEO □ CFO

□ MD □ GM

□ Director □ Manager

□ Assistant Manager □ Supervisor

□ Other_____

Part 2 : General Experian with the origination (item 5-8): *For each question, please put "√" on one answer which is most applicable to you*

5. Has your company been affected by, or at risk for, any of the following business interruptions (Fill in all that apply):

□ Natural Disaster □ Hardware Failure □ Software Failure □Human Error

□ Power Outage □ Service Provider Failure

□Other_____

6. How seriously is crisis business interrupts taken at your organization?

□ Not at all □ Low □ Moderately □ Very □ Extremely

7. How frequently your organization faces the interruption per year?

□ 0-1 times □ more than 1-3 times □ more than 3-5 times

□ More than 5 times

8. What is the expected recovery time for your critical business functions?

□ 0-4 hours
□ 4-8 hours
□ Within one day
□ 1-2 days
□ More than 2 days
□ NA
□ Other_____

Part 3: What important factors that your organization operates.

The following statements have been designed to obtain your opinion on several aspects of business continuity and disaster recovery. For each statement, please indicate the extent to which you agree or disagree with the statement by ticking (√) an appropriate number on the 5 point scale provided. If you totally agree with the statement, tick 5; if you totally disagree with the statement, tick 1.

Factors		**Level of Agreement**				
Business Continuity Plan		**Totally Agree**	**Agree**	**Fairly**	**Disagree**	**Totally Disagree**
9	Organization should prepare for disaster	5	4	3	2	1
10	Organization should have more than one business continuity plan	5	4	3	2	1
11	Documented crisis planning management process has to be within organization policy	5	4	3	2	1
12	Organization should have a dedicated team of professionals focused on business continuity	5	4	3	2	1
13	A good Business Continuity plan can help the organization to restart faster	5	4	3	2	1

Factors		**Level of Agreement**				
Business Impact Analysis		**Totally Agree**	**Agree**	**Fairly**	**Disagree**	**Totally Disagree**
14	The business impact analysis phase would involve the identification of the functions most critical to ensure business continuity	5	4	3	2	1
15	The better Business Continuity plan be created, the loss less money	5	4	3	2	1
16	The customers will continue with the same company when the company shows a good business continuity plan when the disaster occur (reputation)	5	4	3	2	1
17	The better Business Continuity plan, the better management control	5	4	3	2	1
18	How much organization identified important core of business, the fast organization restart	5	4	3	2	1

Factors		Level of Agreement				
Risk Analysis		**Totally Agree**	**Agree**	**Fairly**	**Disagree**	**Totally Disagree**
19	Risk analysis is the identification of procedures that could possibly prevent or reduce the effect of a disaster	5	4	3	2	1
20	Organization should prepare for the risk by educating their employee	5	4	3	2	1
21	The better Business Continuity plan be created, the well of treat and control risk occur	5	4	3	2	1
22	The better Risk Analysis plan, the better management of share and transfer risk to other organizations (insurance)	5	4	3	2	1
23	How much organization identified risk, the opportunity business can take	5	4	3	2	1

IT Recovery Plan		**Totally Agree**	**Agree**	**Fairly**	**Disagree**	**Totally Disagree**
24	The IT system should be available at first priority to continuity the business	5	4	3	2	1
25	Data recovery has to be chosen as a first step towards a recovery plan	5	4	3	2	1
26	Offside backup is require for business continuity plan	5	4	3	2	1
27	Financial performance and SME budgetary issues are bound to play a role when it comes to choosing an appropriate backup strategy	5	4	3	2	1
28	The recovery of IT systems and applications needed by the various business functions	5	4	3	2	1

Testing and Revising		**Totally Agree**	**Agree**	**Fairly**	**Disagree**	**Totally Disagree**
29	Business Continuity plan or Disaster Recovery should test at least one time a year	5	4	3	2	1
30	Test and revising of contingency plan make the plan up-to-date	5	4	3	2	1
31	Testing programs help employees know where to go for information and what to expect in a crisis	5	4	3	2	1
32	Every employee should involve Business Continuity plan or Disaster Recovery testing	5	4	3	2	1
33	Test and revising help organization identify flaws in the plan	5	4	3	2	1

34. Please rate "What do you think that **the Business Continuity Management is important for organization**" by ticking (√) an appropriate number on the 5 point scale provided. If you think it's very important tick 5, unimportant tick 1.

 **1** **2** **3** **4** **5** 

***End of question, Thank you for your cooperation! ***

BIOGRAPHY

NAME		SULIT SANGSUE
DATE OF BIRHT		20 NOVERBER 1986
EDUCATION		
YEAR	**2013**	**MASTER DEGREE**
		Master of Business Administration, Stamford International University (STIU), Thailand
		Scholarship Donor : Stamford International University
YEAR	**2006-2009**	**BACHELOR DEGREE**
		Bachelor of Science, Information Technology, Stamford International University (STIU), Thailand
NATIONALITY		THAI
HOME ADDRESS		49/7 M4 BANGKOK, THAILAND
EMPLOYMENT ADDRESS		AIT, THAILAND
POSITION		NETWORK ENGINEER
EMAIL ADDRESS		SULIT.S@STAMFORD.EDU