ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF IT DISASTER RECOVERY PRACTICES IN ETHIOPIAN COMMERCIAL BANKS

NIGUSSIE BERHANU

JUNE, 2017

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF IT DISASTER RECOVERY PRACTICES IN ETHIOPIAN COMMERCIAL BANKS

A Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By

NIGUSSIE BERHANU

JUNE, 2017

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF IT DISASTER RECOVERY PRACTICES IN ETHIOPIAN COMMERCIAL BANKS

By

NIGUSSIE BERHANU

Name and Signatures of Members of the Examining Board

Name	**Title**	**Signature**	**Date**
Mr. Getachew Jemaneh	Advisor	_____	_____
Dr. Dereje Teferi	Examiner	_____	_____
Dr. Lemma Lessa	Examiner	_____	_____

DECLARATION

I declare that the thesis is my original work and has not been presented for a degree in any other university.

Signature _____

Date_____

This thesis has been submitted for examination with my approval as university advisor.

Mr. Getachew Jemaneh (Advisor)

Signature _____

Date_____

ABSTRACT

The banking industry is highly reliant on Information Technology to provide efficient and timely services to customers. IT play major role in delivering ubiquitous services regardless of time and space in today's highly competitive business environment. As rivals in the banking services are increasing customers would be uncomfortable with any kind of service interruptions. Intolerable services interruptions and sabotages would damage a given bank's public image making its competitiveness questionable in the long run. Banks need to consider strategic plans on how to make their services seamless even at the time of unpredictable incidents and disasters. They need to have contingency plan in place for restoring the IT services and programs that support the underlying mission critical business functions. The purpose of this study is to assess IT disaster recovery practices of Ethiopian commercial banks. The study employed qualitative method to investigate the IT disaster recovery practices and preparedness in 18 Ethiopian commercial banks. A total of 72 participants comprising 54 respondents with relevant expertise and 18 IT managers were selected for the study using purposive (non-probability) sampling. Data was collected through questionnaires and semi-structured interviews, and analyzed using IBM SPSS Version 23 and Microsoft Office Excel 2007. The results of the analysis were displayed using frequency tables, pie charts and bar graphs. The results of the study show that 75.23% of the respondents analyzed both risks that threaten their business and the impacts they would pose on the business. However only half(51.04%) of the respondents agreed that they have risk limitation mechanism in place. 60.4 % of the respondents have IT disaster recovery plan where as the human aspect of IT disaster recovery planning, plan testing and updating are identified to be components overlooked by the banks. Regarding alternate processing site, majority of the responses(38.1%) indicate the use of cold site followed by hot site (14.3%) and warm site (12%). RAID system, cooling, power and connectivity redundancy, and virtualization constitute the top three system protection and resilience solutions the banks have in place with 73.58%, 66.04% and 60.38% of respondents respectively. None of the banks have considered international standards during IT disaster recovery developments. So as to address the observed gaps and weaknesses, the top management needs to regularly oversee implementation, update and testing of IT disaster recovery planning and preparedness in response to emerging threats.

ACKNOWLEDGMENTS

Glory be to God who gave me the strength during this tough time. I would like to thank all the respondents to my research questions for taking their precious time to participate in this research. I would also like to thank Mr. Getachew Jemaneh and Dr. Gashaw Kebede for their valuable guidance without which this thesis work would have not been realized.

Finally, I am grateful to my coworkers especially Yishak Yilma and others for all the unstated supports.

TABLE OF CONTENT

ABSTRACT i
ACKNOWLEDGMENTS ii
LIST OF TABLES v
LIST OF FIGURES vi
ACRONYMS vii
CHAPTER ONE: INTRODUCTION 1
1.1 Background 1
1.1.1Background of Ethiopian Financial Sector 9
1.1.2 Developments in Ethiopian Commercial Banks 9
1.1.3 Resource Mobilization 10
1.1.4 Performance of Ethiopian Commercial Banks 10
1.2 Statement of the Problem 11
1.3 Objective of the Study 12
1.3.1 General Objective: 12
1.3.2 Specific Objectives: 12
1.4 Research Questions 12
1.5 Significance of the Study 13
1.6 Organization of the Study 13
CHAPTER TWO: LITERATURE REVIEW 14
2.1 Business Continuity and Disaster Recovery 14
2.1.1 Business Continuity 15
2.1.2 Business Continuity Planning 16
2.1.3ITDisaster Recovery 16
2.2 Risk Management Regulatory Compliance 18
2.2.1 Global Compliance 19
2.2.2 National Compliance 20
2.3 The IT Disaster Recovery Planning Project 21
2.3.1 Project Initiation 21
2.3.2 Risk and Vulnerability Assessment 21
2.3.3 Business Impact Analysis 24

2.3.4 Mapping Critical Functions to IT Systems 26
2.3.5 IT Disaster Recovery Plan Development 26
2.4 Risk Treatment Strategy Development 29
2.5 Alternate Processing Sites 40
2.6 Chapter Summary 41
CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY 42
3.1 Overview 42
3.2 Research Design 42
3.3 Sampling Design 42
3.4 Location where the Study is Conducted 43
3.5 Data Sources 43
3.6 Data Collection Technique 44
3.7 Questionnaire Administration 44
3.8 Semi-structured Interviews Administration 44
3.9 Data Processing and Analysis 45
3.10 Operational Definition of Terms 45
CHAPTER FOUR: DATA ANALYSIS AND RESULTS 46
4.1. Results of the Study 46
4.2. Limitations of the Study 70
4.3 Chapter Summary 70
CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATION 71
5.1 Discussion 71
5.2 Conclusion 73
5.3 Recommendations 74
References 76
LIST OF APPENDIXES 83

LIST OF TABLES

Table 1: Top 10 global economic loss events(2015)……...2
Table 2 : The most common threats company might face…….23
Table 3: Sample application attack vector, security weakness and associated impact……..34
Table 4: Socio-demographic characteristics of respondents in Ethiopian commercial banks, 2017. (n=53)…….47
Table 5: Risk and business impact analysis in Ethiopian commercial banks, 2017. (n=53)…….48
Table 6: Risk limitation in Ethiopian commercial banks, 2017. (n=53)……51
Table 7: IT disaster recovery plan in Ethiopian commercial banks, 2017. (n=53)……54
Table 8: Alternate processing sites in Ethiopian commercial banks, 2017.(n=53)……..……58
Table 9: System protection and resilience in Ethiopian commercial banks, 2017. (n=53)…..….60
Table 10: Data recovery solution in Ethiopian commercial banks, 2017. (n=53)…….……61
Table 11: Mission critical data backup frequency in Ethiopian commercial banks, 2017. (n=53)…….62
Table 12: IT disaster recovery plan review and update in Ethiopian commercial banks, 2017. (n=53)…….63
Table 13: IT disaster recovery test frequency in Ethiopian commercial banks, 2017. (n=53)…….65
Table 14: IT disaster recovery plan testing method in Ethiopian commercial banks, 2017. (n=53)……...66

LIST OF FIGURES

Figure 1: Direct losses from natural disasters, worldwide ……..1
Figure 2: Combined economic loss…….…….5
Figure 3: Mortality……..…….5
Figure 4: Enterprise operations cycle of disaster recovery……..……..17
Figure 5: The elements of risk……...……22
Figure 6: MTD and RTO……...……25
Figure 7: Risk and business impact analysis in Ethiopian commercial banks, 2017. (n=53)……49
Figure 8: Risk limitation in Ethiopian commercial banks, 2017. (n=53)……..52
Figure 9: IT disaster recovery plan in Ethiopian commercial banks, 2017. (n=53)……..…...56
Figure 10: Summarized percent responses of risk and business impact analysis, risk limitation, and IT disaster recovery plan in Ethiopian commercial banks, 2017. (n=53)…….……..57
Figure 11: Alternate processing sites in Ethiopian commercial banks, 2017. (n=53)……...59
Figure 12: System protection and resilience in Ethiopian commercial banks, 2017. (n=53)……60
Figure 13: Data recovery solution in Ethiopian commercial banks, 2017. (n=53)……61
Figure 14: Mission critical data backup frequency in Ethiopian commercial banks, 2017. (n=53)…….62
Figure 15: IT disaster recovery plan review and update in Ethiopian commercial banks, 2017. (n=53)……..……...64
Figure 16: IT disaster recovery test frequency in Ethiopian commercial banks, 2017. (n=53)…….65
Figure 17: IT disaster recovery plan testing method in Ethiopian commercial banks, 2017. (n=53)…….……66

ACRONYMS

BC Business Continuity

BCBS Basel Committee on Banking Supervision

BCP Business Continuity Plan

BIA Business Impact Analysis

DR Disaster Recovery

DRP Disaster Recovery Plan

FDRE Federal Democratic Republic of Ethiopia

MFI Microfinance Institution

MTD Maximum Tolerable Down Time

NBE National Bank of Ethiopia

RPO Recovery Point Objective

RTO Recovery Time Objective

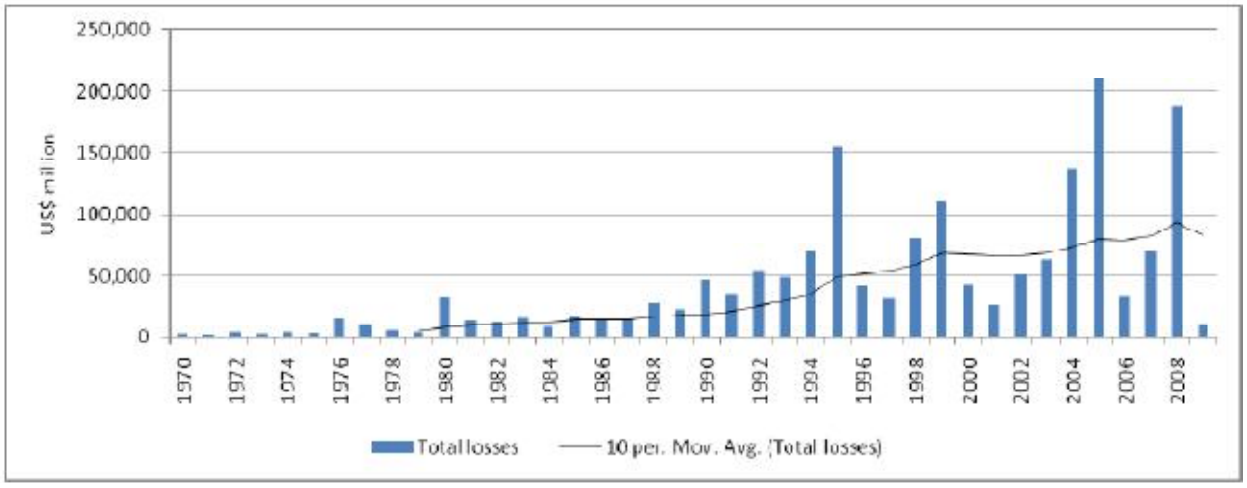
CHAPTER ONE: INTRODUCTION

1.1 Background

Disasters, be it natural or human origin, can cause tremendous economic and life lose. The frequency and intensity of natural disasters with the damages they cause are rising in different parts of the world. “Disaster is a sudden accident or a natural catastrophe that causes great damage or loss of life” (“disaster”,2017, para. 1.).

Economic loss of worth US$ 1 trillion is incurred due to disasters from 2000 to 2010; which accounts for an estimated loss of US$109 billion in 2010 alone. The statistics of the damage in the last two decades is overwhelmingly greater than the earlier decades which may be due to greater exposure, better reporting or both. Unlike the developing countries such as in Africa, the damage is extensive in developed countries such as United States, Europe, and increasingly Asia partly due to the higher value of their infrastructure. The 2005 Indian Ocean tsunami, and Hurricane Katrina in United States cost US$10 billion and US$130 billion respectively. In average, the costs incurred due to disasters in a highly developed nation is US$636 million, a medium-developed nation US$209 million and low-income nation US$79 million(Brigitte, Tim, & Mark, n.d., p.24).

Figure 1: Direct losses from natural disasters, worldwide



(Francis & Olivier, 2010,p.3).

According to Anup(2011), the 9 richter scale measuring earthquake and the resulting tsunami that hit coast of Japan in 2011 was among the greatest magnitudes recorded. Northeast of japan was in total destruction taking the lives of many thousands, others missing, and many more becoming homeless or leaving the area("Japan Earthquake", para. 1).

Table 1: Top 10 global economic loss events(2015)

Date(s)	Event	Location	Deaths	Economic Loss (USD)
April 25 & May 12	Earthquake	Nepal	9,120	8.0 billion
April/May	Heatwave	India	2,500	N/A
June 20 – 30	Heatwave	Pakistan	1,233	N/A
June/August	Heatwave	Europe	1,000	N/A
October 1	Landslide	Guatemala	570	N/A
October 26	Earthquake	Afghanistan, Pakistan	403	100 million
Nov. – Dec.	Flooding	India	386	3.0 billion
January	Flooding	Malawi, Mozambique, Madagascar	307	550 million
July – August	Flooding	India, Bangladesh, Pakistan	303	500 million
February 15 – 28	Winter Weather	Afghanistan	247	Millions
		All Other Events	~3,450	110 billion
		Totals	**~19,500**	**123 billion**

(Aon plc, & Impact Forecasting , 2015, p. 2).

Natural disasters caused an estimated total loss of USD123 billion worldwide in 2015, 30% of which is below the 15-year average of USD175 billion. This is the lowest value since 2009 after four consecutive years of declining losses since the record-setting year in 2011. Wind storms in Europe, forest fires, winter storms in united states, flooding in India, the US,UK, and china; earthquake in Nepal, and cyclones in pacific ocean constitute the main events. Heavy thunderstorm, flooding, and wildfire, were the top three dangers which account for overall 59 percent of all economic losses in 2015(Aon plc, & Impact Forecasting ,2015, p. 1).

Government of the Union of Mynamar (2015) also reported that:

> Torrential rains and the onset of Cyclone Komen triggered severe and widespread floods and landslides in July and August 2015 across 12 out of 14 states and regions in Myanmar. The total economic value of the effects of the floods and landslides was estimated to be approximately K 1.942 trillion (US$1.51 billion). Of this, K 792,493 million (US$615.58 million) was attributed to damages and K 1,149,522 million (US$892.90 million) to losses. The total effects would be the equivalent of 3.1 percent of

> Myanmar's gross domestic product (GDP) in 2014/2015. Productive sectors and housing have been the hardest hit sectors accounting for about 90 percent of the total disaster effects. (p. xviii)

As a result of growth and concentration of population and assets in disaster susceptible areas together with climate variability factors, major disasters are causing rising economic costs in developing countries as measured by the effect on GDP(Cummins & Mahul, 2009, p. 1).

On the other hand Francis & Olivier (2010) state that:

> Developing countries are particularly vulnerable to adverse natural events. Advanced economies are generally able to dedicate increasing resources to reducing vulnerability, including enforcement of building codes and retrofitting of lifeline infrastructure. This is rarely the case in developing countries, many of which are going through rapid urbanization without the means to implement effective risk mitigation strategies. Emerging economies are particularly impacted, as they usually experience rapid growth in their asset base (growth in infrastructure and economic activities) before systems can be put in place to adopt appropriate building standards. (p. 3)

Developing countries do not have the capacity to withstand such adverse disasters and not capable to recovery from the damages posed on facilities and infrastructure through re setup and reconstruction. This causes their impact seriously severe in poorer countries(Eduardo & Noy, 2010, p. 30).

Vunganai et al. (n.d.) states seismic activities in eastern and southern African region as follows:

> Eastern and Southern Africa covers a region which is prone to a significant level of seismic hazard due to the presence of the East African rift system. A number of destructive earthquakes, some causing loss to life, have been reported during this century. For example, in Eritrea, the port city of Massawa was destroyed by an earthquake which occurred in 1921.In Ethiopia, they include the 1960 Awasa earthquake (M_S = 6.1), the 1961 Kara Kore earthquake which completely destroyed the town of Majete and severely damaged Kara Kore town, the 1969 Serdo earthquake (M_S = 6.3) in which four people were killed and 24 injured, 1989 Dobigraben earthquake (M_S = 6.5) which destroyed several bridges on the highway connecting the port of Assab to Addis Ababa, the 1983 Wondo Genet and the 1985 Langano earthquakes which caused damage in parts of the main Ethiopian rift.(p. 2)

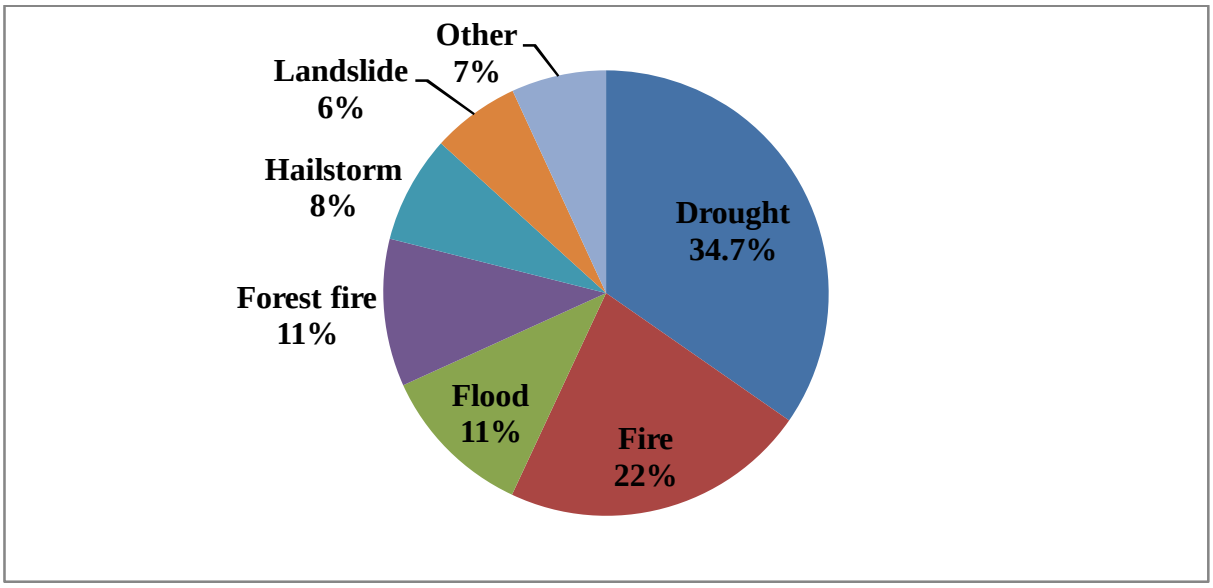
According to Central Intelligence Agency (2017) Ethiopia is a developing and most populous landlocked country in the world with an estimated total population of 102,374,044; The most active and susceptible area to seismic activity is the great rift valley. The most active in regard to recurring volcanic activity in the country is Erta ale with elevation of 613m. Others include Dabbahu(which forced evacuation in 2005 for instance),Alayta, Dalaffilla, Dallol, Dama Ali, Fentale, Kone, MandaHararo, and Manda-Inakir (Geography::Ethiopia, para. 15).

Kinde (2002) described some of the major Ethiopian cities prone to volcanic activities as follows:

> Addis Ababa itself is only 75-100 kilometers away from the western edge of the Main Ethiopian Rift Valley, which is a hotbed of tremors and active volcanoes. Some of Ethiopia's major cities like Addis Ababa, Adama, Dire Dawa and Hawassa are very near main fault lines such as the Wonji fault, the Nazret fault, the Addis-Ambo-Ghedo fault, and the Filwoha fault lines along which numerous earthquakes of varying magnitude have occurred over the years. Other cities like Arba Minch, Dessie, and Mekele are also located in some of the most seismically active areas in the country. The presence of the FilWoha hot springs in the middle of Addis Ababa itself, for example, is nature's reminder that the city lies on fault lines that have been slowly building strains. It is the release of these strains accumulated over the years that cause the phenomenon of earthquake.(p. 1)

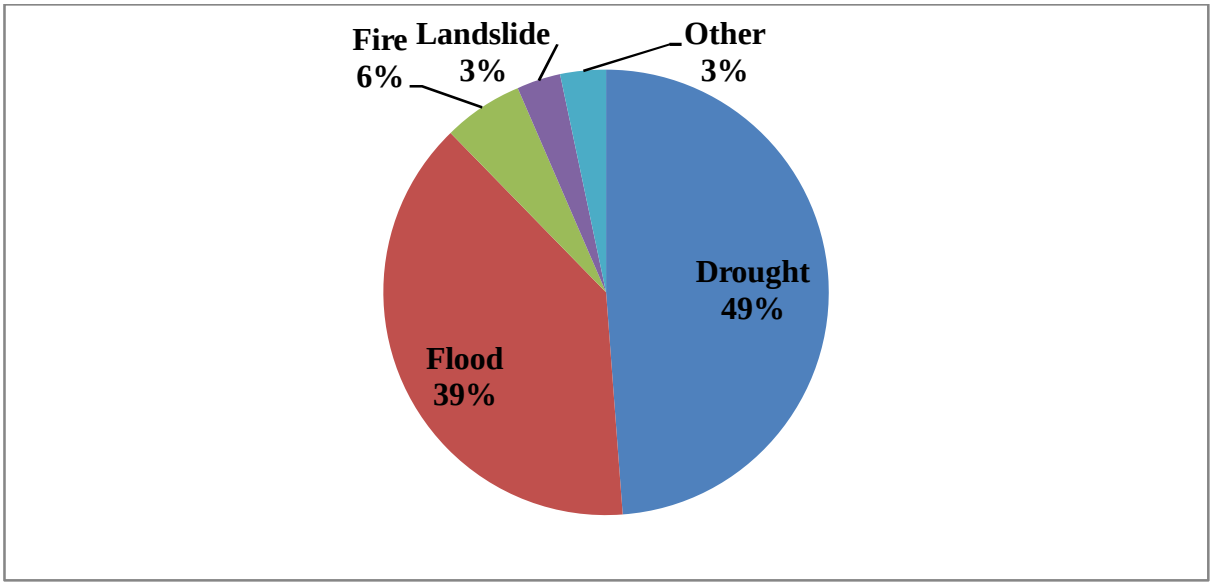
Nationally Reported Losses due to disasters in Ethiopia (1990 – 2014)

Figure 2: Combined economic loss



(UN Office for Disaster Risk Reduction (UNISDR), 2014).

Figure 3: Mortality



(UN Office for Disaster Risk Reduction (UNISDR), 2014).

In addition to natural disasters, man-made disasters pose serious threats and risks to information system assets. Man-made disasters are mainly caused by human error, ignorance, negligence or individuals with malicious intentions. Data breach incidents in which unauthorized people acquire access to or tamper confidential data are also main security concerns today.
Verizon Data Breach Investigation Report of 2015 compiled from incident contributions of 70 organizations from 61 countries all over the world shows that there were 79,790 security incidents, out of which 2,122 are confirmed data breaches. As per the report, top three industries affected are public, information and financial services respectively(ACE et al., 2015, p.1).

According to a survey entitled 'The State of IT Disaster Recovery Amongst UK Businesses' which was conducted by Opinion Matters Inc. (2016), there are varying types of incidents that cause business disruption with some factors hindering the successful failover of operations to disaster recovery site. As per the finding 95% of the survey respondents have faced an outage of some kind in the past 12 months. The issues mainly range from system failure through to human error, corrupted data, and unexplained downtime due to cyber-attacks. According to the report, system failure (53%) and human errors were the two biggest incidents the respondents experienced, which resulted in data loss and downtime (52%). 58% have experienced some failover problems to disaster recovery or have no enough confidence to trigger their disaster recovery(Survey Results, par. 1).

Zetta surveyed 403 IT professionals of 20 companies from different industries in October 2016 with an overall objective of identifying their IT disaster recovery solutions, plans and experiences. Accordingly,

- 96 percent reported that they have IT disaster recovery solution
- 54 percent reported that they have encountered down time greater than 8 hours in the last five years
- Power outages(75%), hardware error(53%) and Human error(35%) were most common causes of IT downtime
- 2 in 5 companies still don't have a documented IT DRP, and 40% only test their IT DRPs once per year
- 40 percent of organizations do not have a formally documented IT disaster recovery plan to guide them in the event of an outage. The same number (40%) of companies test those

IT disaster recovery plans only once annually and IT disaster recovery testing frequency remains inadequate (2016 State of Disaster Recovery Report, (n.d.)).

ReRez research conducted Disaster Preparedness Survey among SMBs (Small and Medium Business) in February and March of 2012. The research was commissioned by Symantec Corporation and the research participants contacted were business and IT executives of 2,053 SMBs in 30 countries. The finding shows that:

- 34 percent of the respondents are implementing or have already deployed server virtualization, of which 71 percent reported improved disaster preparedness because of that deployment and
- 35 percent use mobile devices to access business information (Symantec Corporation, 2012, p. 7-12).

Similarly, ReRez Research contacted business and IT executives at 4,506 organizations in 38 countries to conduct a survey on the state of Information, out of which 2,053 responses came from SMBs. As per the finding, an estimated 40 percent of the worth of SMBs is derived from the information they own. They also responded loss of customers (49 percent), damage to the brand (43 percent), increased expenses (41 percent) and decreased revenue (37 percent) would result if their organizations' information is irrecoverably lost. On the other hand, 65 percent (two third of the businesses) said that they have lost important business information/data due to causes such as human error, hardware failure, software failure and lost or stolen mobile devices where as 91 percent exposed confidential data in the past 12 months. Almost one-fourth of SMBs have had regulatory compliance issues in the past year (Symantec Corporation, 2012, p. 8-10).

According to Sungard Availability Services statistics on UK businesses in 2014,

- Overall business outage in which employees are unable to access mission critical systems increased beyond one third (38 percent) compared to 2013, which is indicative that companies are not sufficiently investing in availability and business continuity strategies and solutions.
- Disruptions due to technology failures have more than doubled, increasing by 140 percent, and
- Hardware failure has been the main issue, causing a fifth of all problems (21 percent). The year-on-year spike in technology-related incidents, also including power and

communications, is particularly worrying when it comes to business disruptions (Are UK business disruptions on the rise?,para. 2-3).

Forty institutions in Addis Ababa that are familiar with the use of ICT including 17 banks, 12 ICT institutions and 6 others such as federal governments, agencies, media, and transport were surveyed in 2015 regarding their cybercrime experiences . According to the report,

- Computer viruses, worms, malware, or other malicious attacks (57.1 %), website defacement (40%), illegal access (17.1%), and spam (14.7%) were the most frequently perpetrated cybercrimes against the institutions
- Damage to computer data (62.9%), denial of service (DOS) (45.7%), and system interference (45.7%) were also infrequently occurring cybercrimes they faced(Hailu, 2015, p. 7-8).This shows that Ethiopia is also facing disasters of both natural and man-made cause that should alert Ethiopian commercial banks to look into their IT disaster recovery preparedness.

Based on data obtained from KSN (Kaspersky Security Network) during the period from July 1st, 2016 to October 1st, 2016, analysis of trends related to financial cyber-attacks, phishing and banking malware, including attacks on mobile devices, POS (Point of Sales) systems and ATMs(Automated Teller Machine) indicates that Ethiopia is the 2nd top and the 7th top country in the world that is attacked by POS malware and banking Trojans respectively(Telefonica,2016, p. 33-50).

In his report of the state of cybercrime governance in Ethiopia, Hailu (2015) also stated that:

> There is no consolidated report that shows the exact prevalence and impact of cybercrime in Ethiopia and to what extent the Ethiopian information society is vulnerable. This is partially due to the fact that companies and individual users do not report cybercrime incidents, do not keep organized records, and, in some cases, are not even aware that they are targeted by cybercriminals. Records from intelligence and law enforcement agencies are often improperly recorded or inaccessible. Ethiopian-specific literature on the extent of cybercrime activities is also nonexistent. The inadequacy of the available statistics could lead to the over- or under-estimation of the threat of cybercrime to Ethiopia. (p.7)

1.1.1Background of Ethiopian Financial Sector

The financial system of Ethiopia constitutes banks, insurance companies and microfinance institutions. According to National Bank of Ethiopia(2012), there are19 licensed commercial banks(16 private banks and 3 government-owned banks), 19 private and 1 government owned insurance companies, and 35 MFIs as of May,2012(History of Banking, para. 21).However as Construction and Business Bank was merged to Commercial Bank of Ethiopia in 2016, the government owned commercial banks are currently reduced to2. In summary, there are16 private commercial banks, 2 government owned commercial banks, and National Bank of Ethiopia-which is the central regulatory body of the other banks operating in the country. See table below for a list of the licensed commercial banks operating in the country:

1.1.2 Developments in Ethiopian Commercial Banks

Banks dominate the Ethiopian financial system with nearly 95% share of assets, 97% share of deposits, 94% share of loans and advances, and 77% equity share of the financial sector on average. Similarly the banking sectors size is rising dramatically over the course of the years in terms of assets, deposits, loans and equities owned (Kassie,2014, p.1).

National Bank of Ethiopia (2014/2015) states the following in terms of the commercial banks' branch expansion:

> The banks opened 485 new branches in 2014/2015(of which 359 were private) raising the total branch network in the country to reach 2693 from 2208 last year. As a result, bank branch to population ratio declined from 1:39,833.8 people to 1:33,448.2 in 2014/15.The significant branch expansion was undertaken by Commercial Bank of Ethiopia(CBE) with 127 branches, followed by Awash International Bank (55 branches), Oromia International Bank(43 branches), United Bank (29 branches), Bank of Abyssinia(27 branches), and Lion International Bank (26 branches). Despite aggressive branch expansion by public banks, their share in total branches slightly went down to 41.9 percent from 45.4 percent last year. About 35.5 percent of bank branches were in Addis Ababa, during the review fiscal year. The total capital of the banking industry increased

by 19.0 percent and reached birr 31.5 billion by the end of June 2015 as a number of banks injected more capital. As a result, the share of private banks in total capital marginally increased to 56.5 percent from 55.4 percent last year, while that of CBE remained at 34.0 percent.(p. 50)

1.1.3 Resource Mobilization

Similarly regarding resources mobilized by the commercial banks, National Bank of Ethiopia (2014/2015) also states that:

> The resources mobilized by the banking system in the form of deposit, loan collection and borrowing increased by 24.5 percent and reached Birr 138.7 billion at the end of 2014/15. Spurred by remarkable branch expansion, deposit liabilities of the banking system reached Birr 367.4 billion reflecting annual growth rate of 25.5 percent over last year. Component wise, time deposits registered significant increase (131.6 percent) followed by saving deposits (19.8 percent), and demand deposits (16.8 percent). Saving deposits accounted for 47.6 percent of the total deposits followed by demand deposits (41.0 percent) and time deposit (11.5 percent). The rise in saving deposits indicates the steady growth in financial intermediation of banks. The share of private banks in deposit mobilization increased only marginally to 32.2 percent from 31.5 percent last year despite their opening of 359 new branches. CBE alone mobilized 66.1 percent of the total deposits due to its large branch network. (p. 54 - 55)

1.1.4 Performance of Ethiopian Commercial Banks

With respect to financial sector performance, Ethiopia has made remarkable progress. Commercial banks opened 485 new branches which increased their total to 2,693 up from 2,208 a year ago. Commercial banks on their part have stepped up their deposit mobilization which saw a 25.5 percent annual growth. Their loan collection exhibited a 16.0 percent increase and new loan disbursement about 26 percent expansions. of the total new disbursement, about 68 percent

went to finance private sector. Moreover, all indicators showed that commercial banks were well capitalized and their returns on equity and assets were well above the required level, and their non-performing loans were kept within the prudential requirement (National Bank of Ethiopia, 2014/2015, p. 3-4).

The findings of Modeling and Analysis of Ethiopian Banking Sector Performance using BSC and AHP Approaches as indicated by Diriba (2015) shows that Commercial Bank of Ethiopia(CBE) ranked first with the score of 34.47%, followed by Awash International Bank(AIB) (19.82%) which performed slightly better than Dashen Bank(DB) (19.49%) and standing fourth is Oromia International Bank(OIB) (14.87%) and occupying the last position was Addis International Bank(AdIB)(11.36%) in terms of performance as rated by experts in contrast based on conventional ratio analysis AdIB stood first with a score of 78% followed by OIB at 63%, then AIB (58%) and the fourth place belonged to CBE (51%) and finally DB (50%)(p. 48).

1.2 Statement of the Problem

I have personally witnessed in my office that recovery process from unexpected failure of applications installed on VMware has increased a bank's downtime due to lack of appropriate disaster recovery plan that should have guided the recovery procedure. There had to be a structured way to continue business and restore operations in the event of such a sudden business outage. Ad-hoc recovery tasks of such service disruptions create psychological pressure even on staffs that might have the technical skills required unless there is some sort of documented plan that will aid them in getting directions and concentration. Such ad-hoc recovery procedures risk the bank unnecessary service downtime, degraded public image, and ultimately customer frustration.

Thus, Commercial Banks in Ethiopia have to make sure that they are not in a position to spontaneously react to such IT disasters after they have happened but need to have recovery plans in place to guide the necessary procedures to undertake. Such plans are also expected to comply to international standards of business continuity and disaster recovery guidelines to ensure their effectiveness.

1.3 Objective of the Study

The aim of this study is to assess the current IT disaster recovery practices and preparedness of Ethiopian commercial banks with the following general and specific objectives.

1.3.1 General Objective:

The general objective of this research is to assess the IT disaster recovery practices of Ethiopian commercial banks.

1.3.2 Specific Objectives:

- Find out if the banks have IT Risk limitation mechanisms put in place
- Investigate if commercial banks have performed business impact analysis to identify mission critical applications
- For commercial banks that have IT DR plans, evaluate their plans to determine if there is gap they should address and also investigate if the plans are regularly tested and updated in response to technological and procedural changes.

1.4 Research Questions

The following research questions are addressed in this study:

- To what extent are risks to IT systems and services limited?
- What is commercial banks' practices regarding IT Disaster Recovery planning, maintenance and testing?
- Which components of IT disaster recovery preparedness are overlooked?
- What percentage of commercial banks has alternate processing sites?

1.5 Significance of the Study

The study provides insight in to current IT disaster recovery practices of Ethiopian commercial banks and produces an input for policy makers to fill any observed gaps. The finding will also help the respective bank managements revise IT components of their business continuity strategies and follow-up their implementations according to the standardized modes of disaster recovery practices

1.6 Organization of the Study

This thesis constitutes five chapters. The first chapter is Introduction and contains background of Ethiopian financial sectors, research questions, objectives and significance of the study. The second chapter is literature review which provides both conceptual and contextual ground in the existing body of knowledge related to business continuity and IT disaster recovery. The third chapter presents the research design and methodology used in this study. In chapter four, the data gathered from research participants is analyzed and its results are presented. Discussion, conclusion and recommendations are presented in the final chapter which is chapter five.

CHAPTER TWO: LITERATURE REVIEW

2.1 Business Continuity and Disaster Recovery

Banking industry is at the forefront in adopting state of the art Information and Communication Technology services for efficient, timely and reliable banking services to its customers. Implementation of technology also enables it to expand its market beyond geographical limitations to be competitive in a global market. On the other hand, News of unprecedented natural and human-made disasters across the world is becoming part of our day to day life which poses the availability of such financial industries at risk. Such events cause major and unprecedented business disruptions, life and economic losses. Recent acts of terrorism in Istanbul, New York, Madrid, London and elsewhere, and even outbreaks of pandemic diseases that affect workforces are beyond warning signals for businesses to check how prepared they are to survive such disasters.

After examining and quantifying the impact of New York City September 11th attack on each industry sector, it was found out that financial services, tourism and retail sectors felt the greatest impact; small businesses in all sectors were and will continue to be the hardest hit. Based on the findings , it was identified that priorities that must be addressed by the sectors include restoring confidence by investing in comprehensive, innovative security measures; Executing a five-borough strategy to retain and expand the financial services industry, and senior management of every business has had to reevaluate the geographic concentration of their talent and facilities, security, space needs and data and phone systems(New York City Partnership and Chamber of Commerce, 2001, p.5).

The September 11, 2001 attack revealed that the level of disaster recovery preparedness varied among different organizations. The financial industry made great effort in business continuity and disaster recovery planning tasks when it comes to data systems. Cantor Fitzgerald had redundant systems and as a result it overcame the impact of the disaster unlike smaller

companies such as Sandler O'Neill that were less prepared and thus forced to rebuild their IT systems from the scratch. Above all, it was apparent that the loss of human capital including the recovery team itself as a result of the disaster was heartbreaking(Thomas, 2009, p. E2.1).

Business continuity and disaster recovery (BC/DR) plans were certainly put to the test by many financial firms after the terrorist attacks in the United States on September 11, 2001; but even six years later, there are many firms that still do not have any type of business continuity or disaster recovery plan in place. It seems insane not to have such a plan in place, but statistics show that many companies don't even have solid data backup plans in place due to Lack of time, resources, sense of urgency and lack of a process for developing and maintaining a plan(Susan, 2007, p.2).

The pressures of regulatory compliance requirements, competition in the financial industry and the ever growing threats forced financial institutions to consider and develop thorough contingency plans to ensure business continuity. A carefully developed, trained and well tested Business Continuity Plan (BCP) is the best method to ensure business availability at the time unprecedented disasters(Daniel, 2011, p. v).

The factors stated above have forced the financial industry and businesses to look into their business continuity and any workaround to follow for their business operation to render the required mission critical services to its target customers at the time of disaster.

2.1.1 Business Continuity

Basel Committee on Banking Supervision (2006) defines Business Continuity as "a state of continued, uninterrupted operation of a business"(p.1). Business continuity keeps a company operating regardless of any potential threat that causes disruption to its normal day to day operation. This is to mean the business has to continue operating no matter what. There are three main dimensions in today's typical business company. These are people, technology and process. People carry out process through the use of technology. Any intentional or unintentional misuse of a given company's information system or asset by its own internal employee can cause a major damage to the company. Hence a business continuity plan has to consider the aforementioned three components(Susan, 2007, p.5).

2.1.2 Business Continuity Planning

Business continuity planning (BCP) is a methodology that a given company sticks to in order to keep the business running before, during and after disasters and disruptive events(Susan, 2007, p. 3).

Marianne , Pauline, Amy, Dean, and David (2010) argued that:

> The BCP focuses on sustaining an organization's mission/business processes during and after a disruption. An example of a mission/business process may be an organization's payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.(p.8)

Business continuity creates a way to sustain its normal operations in event of disasters. By creating an accurate plan to mitigate impact, business continuity develops guidelines and procedures to follow when applications fail or network systems are down. There are back up software and solutions to easily restore the normal functions of people and equipment.

2.1.3 ITDisaster Recovery

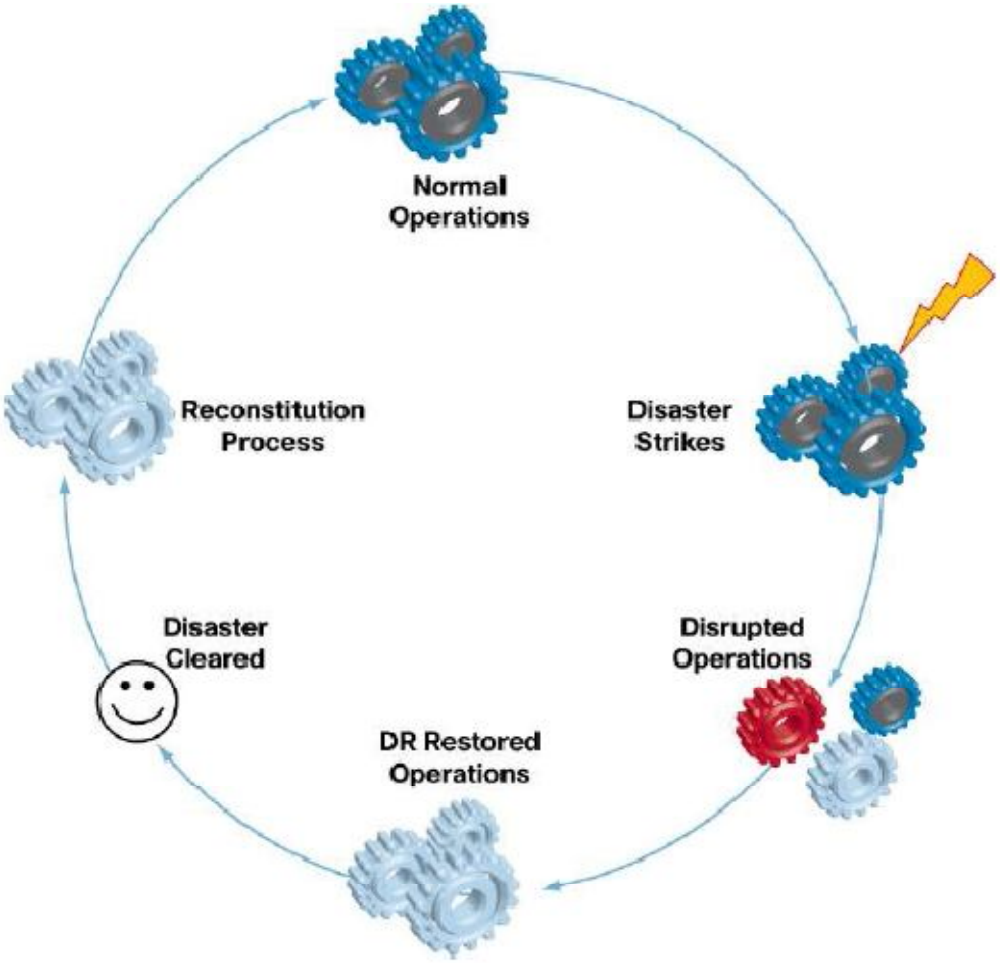
Susan(2007) stated that "IT Disaster recovery is part of business continuity, and deals with the immediate impact of an event. For example, recovering from a server outage and security breach falls into this category" (p. 4). It is a business's ability to get back to track after a disaster hits by restoring IT systems and services operations to the same /nearly the same state they were in before the disaster occurred.

Business Continuity Planning (n.d.) explains disaster recovery and disaster recovery plan as follows:

> Disaster Recovery is the process an organization uses to recover access to their software, data, and/or hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans. Disaster recovery plans guide the procedures in recovering all the lost data and

information. This also includes other investments and lost physical assets that may disrupt the operations of the business. While Disaster Recovery plans, or DRPs, often focus on bridging the gap where data, software, or hardware have been damaged or lost, one cannot forget the vital element of manpower that composes much of any organization. A building fire might predominantly affect vital data storage; whereas an epidemic illness is more likely to have an effect on staffing. Both types of disaster need to be considered when creating a DR Plan. Thus, organizations should include in their DRPs contingencies for how they will cope with the sudden and/or unexpected loss of key personnel as well as how to recover their data(Disaster Recovery, para. 1).

Figure 4: Enterprise operations cycle of disaster recovery



(Cisco Systems, 2008, p.4).

Similarly according to Business Continuity Planning (n.d.),

> Disaster Recovery Plans, being part of a larger and more extensive practice known as Business Continuity Planning, should be well practiced so that the key players are familiar with the specific actions they will need to take should a disaster occur. DR plans must also be adaptable and routinely updated, e.g. if new people, a new branch office, or new hardware or software are added to an organization they should promptly be incorporated into the organization's disaster recovery plan. Companies must consider all these facets of their organization as well as update and practice their plan if they want to maximize their recovery after a disaster(Disaster Recovery, para. 2).

It is a way of stopping the post disruptive effects of the disaster as soon as possible and focusing on the resolution. It could be disconnection or turning off the systems that have been breached, performing damage assessment of facilities impacted by flood or earthquake and deciding on the best solution to be taken(Susan, 2007).

In a general term, both business continuity and disaster recovery are meant to preserve the business operation.

2.2 Risk Management Regulatory Compliance

Kalus(2006) describes the nature of risk management regulatory compliance requirement as follows:

> Most compliance demands have two things in common: they demand that some behavior is followed and documented, and that risk is managed proactively. Risk management of business processes focuses on financial operations first, but IT services are not far behind owing to their importance for most business processes. Ensuring availability of IT services, both short and long term, is therefore important for regulatory compliance as well. (p.17)

On the other hand Eric and William (2002) stated that:

> Many companies are regulated by federal, state, and local statutes. As more companies utilize information technology as a core part of their business operations, there are more regulations specifically aimed at ensuring that information is appropriately protected. Without doubt the most regulated are the financial services and medical industries. These

> industries have long had requirements for protecting the privacy of customer and patient data. With the increased usage and dependence on information systems and networks, the government has begun to pass legislation specifically aimed at controlling access to and protecting the confidentiality of such information. (p. 19)

James, Mike, and Darril (2015) state that "In many countries, financial institutions, such as banks and the firms that process their data, are subject to strict government and international banking and securities regulations designed to facilitate their continued operation to ensure the viability of the national economy"(p. 143).Having robust business continuity plan in place helps the banking industry to ensure customer confidence and also to attract new clients. It has to be ensured that information security program helps the company stay compliant with all relevant regulations.

2.2.1 Global Compliance

The Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) has put very specific requirements on the way financial services firms protect information. It requires formal information security programs to be established and recognized by senior management. The GLBA states that the board of directors must approve the information security plan. These new regulations are forcing organizations to create formal information security programs and spend money to ensure they are adequately protecting information systems (Eric & William, 2002, p. 19).

Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (BCBS) is the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability. The BCBS does not possess any formal supranational authority. Its decisions do not have legal force. Rather, the BCBS relies on its members' commitments to achieve its mandate. BCBS members include organizations with direct banking supervisory authority and central banks.

The Basel Committee's work

According to Bank for International Settlements (2016),

The core of the work undertaken by the Basel Committee focuses on the following activities:

- Exchanging information on developments in the banking sector and financial markets to help identify current or emerging risks for the global financial system
- Sharing supervisory issues, approaches and techniques to promote common understanding and to improve cross-border cooperation
- Establishing and promoting global standards for the regulation and supervision of banks, as well as guidelines and sound practices
- Addressing regulatory and supervisory gaps that pose risks to financial stability
- Monitoring the implementation of BCBS standards in member countries and beyond to encourage their timely, consistent and effective implementation
- Consulting with central banks and bank supervisory authorities which are not members of the BCBS to benefit from their input into the BCBS policy formulation process and to promote the implementation of BCBS standards, guidelines and sound practices beyond BCBS member countries
- Coordinating and cooperating with other financial sector standard setters and international bodies, particularly those involved in promoting financial stability(The Basel Committee's Work, para. 1).

2.2.2 National Compliance

National Bank of Ethiopia

The National Bank of Ethiopia (NBE) incorporated latest developments in the areas of risk management practices in to regulatory compliance requirement guideline making it consistent with international standards and best practices. The guideline covers the most common and interrelated risks facing banks in the country, namely, credit, liquidity, market and operational risks.

Operational risk, as stated by NBE, includes the exposure to loss resulting from the failure of a manual or automated system to process, produce or analyze transactions in an accurate, timely

and secure manner. IT, legal, regulatory, strategic, reputational, and systemic risks are categorized under operational risk. According to the guide line, board of directors shall develop an overall risk management strategy and policies to be executed by the respective business functions. The senior management at each business functions shall design procedures to control and monitor risks in conformity to the overall risk management strategy. Commercial banks are also expected to notify NBE regarding any update to their risk management programs within 15 days of its effective date (Bank Supervision Directorate, 2010,p.31).

2.3 The IT Disaster Recovery Planning Project

2.3.1 Project Initiation

Project initiation phase of IT disaster recovery planning project is described by Susan(2007)as follows:

> Project initiation is one of the most important elements in BC/DR planning, because without full organizational support, the plan will be incomplete. As an IT professional, there may be limits to what can be done to create an organization wide functional BC/DR plan. For example, permissions for a particular business application may be set, but is it really known how users interact with it and what would be required to get the business back up and running with regard to that particular business function? If the application server is destroyed and data backups are available, does a backup server exist? Is there a way to allow users to connect to the application securely? Where are users located? How will business resume? Can it resume without that application in the near-term or not? These will likely be not answered questions. It requires the input and assessment from subject matter experts in other departments and divisions. Therefore, getting executive and companywide support for the BC/DR planning process is absolutely key to its success. (p.33)

2.3.2 Risk and Vulnerability Assessment

Risk is “a situation involving exposure to danger; The possibility that something unpleasant or unwelcome will happen; A person or thing regarded as a threat or likely source of

danger”(“risk”,2017, para. 1.).No organization open to external world is risk free. All possible risks that a business faces must be assessed and a strategy to reduce their impact has to be established. Risk identification is drawing up a comprehensive list of the events that can be a threat to an organization. Periodic information published by local or state government agencies that work on disaster management can be consulted for disaster frequencies and likelihoods relevant to an area. Risks will arise when there is any possibility that environmental threats take advantage of existing vulnerabilities in day-to-day business operations, assets or facilities.

Figure 5: The elements of risk

(James et al., 2015, p.106).

Table 2 :The most common threats company might face

Natural Risks	Man-Made
Earthquake	Terrorism
Flood	Sabotage / vandalism
Tornado	Cyber attack
Hurricane	Social engineering
Land slide	Causing Fire
Fire	Errors

Gerard (n.d.) defines disaster recovery planning inclusive of vulnerability assessment as follows:

> Disaster recovery planning (sometimes also called a business process contingency plan) is a process inclusive of a business vulnerability assessment, development of a disaster recovery framework, a written disaster recovery plan encompassing the recovery strategies, and advance information system in conveying DRP. The purpose of vulnerability assessment is to determine the relative monetary and functional contribution of the business, and its business interruption, and impact analysis.(p.88)

All potential risks to operation of the business are analyzed possibly with the help of risk modeling tools. The risks can be investigated from two perspectives: risk source and assets. Risk sources in this case are any threat sources, e.g online attackers, that may pose threat to systems and infrastructures. With this regard the attackers behaviors and intentions are closely monitored and learnt so as to implement mitigation strategies. In case of asset, its vulnerability at each layer is assessed in terms of access controls, protocols, applications and networks. As part of the risk analysis procedure, the likelihood assessment of each potential threat is also identified which is the number of times you expect it to disrupt the business each year (James et al.,2015, p.74).

2.3.3 Business Impact Analysis

2.3.3.1 Impact Criteria

The following is recommendation from International Organization for Standardization (2008) on how to develop and specify impact criteria:

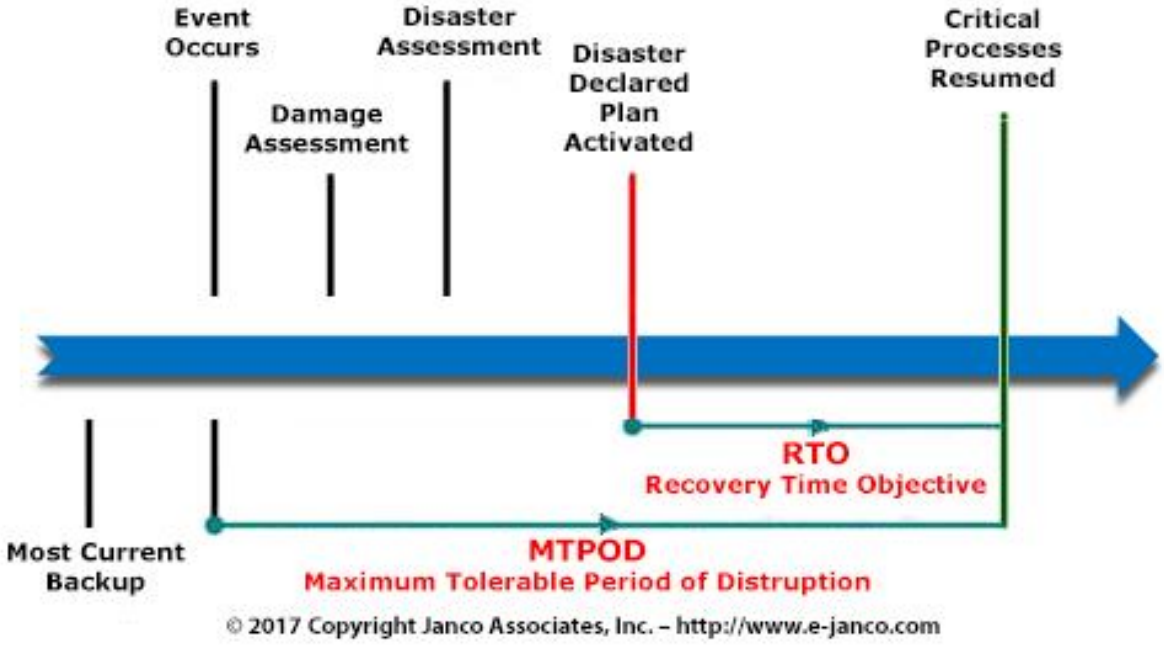
> Impact criteria should be developed and specified in terms of the degree of damage or costs to the organization caused by an information security event considering the following:
>
> - Level of classification of the impacted information asset
> - Breaches of information security (e.g loss of confidentiality , integrity and availability)
> - Impaired operations (internal or third parties)
> - Loss of business and financial value
> - Disruption of plants and deadlines
> - Damage of reputation
> - Breaches of legal, regulatory or contractual requirements. (p. 8)

In Impact analysis phase, you analyze the data gathered during risk identification and likelihood assessment and attempt to determine what impact(cost of damage) each one of the identified risks would have on the business if it were to occur. This could be calculated in terms of percentage of the asset destroyed(lost) per disaster and monetary value lost on the asset per disaster . The monetary value lost could be estimated as total worth of the asset * percent of the asset lost due to the disaster. The annual loss expectancy due to this particular disaster can be estimated as monetary value lost per a disaster hit *the disaster's expected annual frequency in the area. Note that a given disaster's annual frequency of occurrence is estimated in likelihood assessment phase of risk analysis (James et al., 2015, p. 149-150).

Following the risk and vulnerability assessment phases, the Recovery Time Objective (RTO) , Maximum Tolerable Downtime(MTD) also called Maximum Tolerable Period of Disruption(MTPOD) and Recovery Point Objective (RPO) values set for mission critical

business applications are used to develop a disaster recovery framework. The RTO entails how long the intervals between the disaster and post-disaster resumption of function to restore data actually take, while RPO describes how current the data has to be(Gerard, n.d., p.88).

Figure 6: MTD and RTO



2.3.3.2 Resource Prioritization

From a quantitative point of view, this process is relatively straightforward. You simply create a list of all the risks you analyzed during the BIA process and sort them in descending order according to the annual loss expectancy computed during the impact assessment phase. This all steps sum up to risk analysis - examining an environment for risks, evaluating each threat event as to its likelihood of occurring and the cost of the damage it would cause if it did occur, assessing the cost of various countermeasures for each risk, and creating a cost/benefit report for safeguards to present to upper management(James et al.,2015, p.151).

It is to be noted that the successful investigation of risks that a company faces and the impacts the risks would pose on the company requires coordinated engagement of all stakeholders and concerned parties in the organization. Communication, Information Technology, company

structure, management commitment, culture, training and trust are the seven success factors to increase the effectiveness of risk management procedures (Prapawadee & Wariya, 2009, p.iii).

2.3.4 Mapping Critical Functions to IT Systems

The importance of IT services and IT systems is directly related to their business relevance. It depends on the revenue, which depends on their functionality, or on the amount of damage in case of an outage, or if there are regulations that demand their functionality. Since the importance of service varies a lot, the importance of their failures and service outage are quite different too. As far as business processes depend on IT services, we have to manage their underlying IT service continuity.

As Kalus (2006) states:

> IT outages affect either revenues or costs and we either can determine the effect directly or we can estimate it. If a given point of sales systems is down, or if a company sells goods or services on the Internet, any outage in these systems will cause customers to go to competitors whose systems are still working. In the long term, many customer-visible system outages will damage the company's reputation and will result in loss of clients.(p. 15).

2.3.5 IT Disaster Recovery Plan Development

The list of procedures and activities to be undertaken to restore operations and put the interrupted business back on track requires planning in advance.

Grand Forks states that fruitful disaster management is a result of thorough planning ahead, training and joint venture , persistent communication and teamwork(as cited in Brenda, 2009, p.62).

2.3.5.1 Planning User Workstation Recovery

Various aspects of recovering user workstations include web terminals (primarily used just as a Web browser), client-side applications and tools, access to centrally located information; and recovering users' communication needs, including voice communications, e-mail, fax and instant messaging (IM). Recovering these capabilities requires recovery plans that quickly restore users' ability to perform their tasks and support critical business processes(Peter, 2008,p. 97).

2.3.5.2 Planning Facilities Protection and Recovery

Facilities in this context focus mainly on information processing facilities such as data centers. Physical access control, Electric power protection, Fire detection and suppression systems, protection against chemical hazards and water/flooding detection are some of preliminary measures of protecting a company's information processing facilities. This phase of the IT disaster recovery plan development has to also consider specification of the type and where about of an alternate processing site to take over the functions of primary processing site during disasters(Peter, 2008, p. 130).

2.3.5.3 Planning System and Network Recovery

Step by step procedures for restoring networks and systems should be part of the IT disaster recovery plan. The instructions have to be so clear that even an IT personnel with minimal expertise on the area is able to restore a particular service just by closely following the instructions specified in the plan.

A case study involving four companies based in the Western Cape was conducted. These companies were chosen because each of them has a BCP in place and each have experienced prolonged downtime during a disaster. The reason for the prolonged downtime ,as per the researcher's finding is that certain crucial aspects such as the network routers, network connections and software application services within their BCP has been overlooked and thus could not be implemented, causing them to have prolonged downtime during disasters(Mogamat, 2012, p. 17).

Teams responsible for the restoration of vital IT systems have to be identified and take the mandate accordingly. It is recommended that personnel with better expertise on each area have to be identified and equipped with better training.

2.3.5.4 Planning Data Protection and Recovery

In this age of knowledge based economy, business data is the greatest asset a company can have especially when it comes to commercial banks. It is imperative to have a systematic protection and recovery mechanism in place. Some of data protection mechanisms include physical access

control, access authentication & authorization, encryption, deployment of in-depth defense security technologies (hardware/software) and staff training. Properly configured backup systems, mirroring and replication technologies can ensure safety of business data at time of uncontrolled disasters. Furthermore, planning on data protection and recovery mechanisms ahead also saves banks from unnecessary expenses incurred due to legal measures

2.3.5.5 Writing the DR Plan

The step at this point is writing down the disaster recovery plan according to the plan components addressed above. All necessary recovery procedures with the target responsible teams for the recovery have to be clearly written down in the plan document. Document management packages provide tools and features to build a professional document in this regard, It is also advisable to track changes to the document through the use of revision numbers.

2.3.5.6 Training and Testing

Malssen(2006) states that "A well-practiced plan will create a rational framework that can guide staff members through difficult and confusing situations, keeping in mind that the situation will vary with each incident" (p. 6).

Finding of an empirical research where data was collected through a questionnaire from IT executives involved in Disaster Recovery from the 11 domestic commercial banks of srilanka shows that the banks are weak in the areas of Disaster Recovery Plan Testing and Maintenance. (Fernando, 2008, p. iii).

A well-developed plan without proportionate training and testing is not so important than giving a false sense of security. Testing helps to identify anything overlooked in the plan component that might be a potential bottleneck in the disaster recovery effort. Hence it gives an opportunity to correct and maintain the plan accordingly. The disaster recovery team has to have a complete mental image of what to do when unprecedented disaster hits. This is attained through extensive training of the disaster recovery plan on how to use and comply to the plan.

2.3.5.7 Plan Maintenance

The plan has to be regularly maintained and updated to reflect any changing technology and business procedures. The plan that works today might not work tomorrow as the day brings its own variables in to the business environment. Therefore, the plan has to be modified and tested accordingly in order to sustain the company's confidence.

2.4 Risk Treatment Strategy Development

The costs of all available options of risk mitigation strategies have to be evaluated against the damage the risks may pose on assets and the feasible one must be selected for implementation. Gaps in proper evaluation and response to potential risks place an organization in high vulnerability.

Types of Risk Treatment Strategies

The four standard choices of risk mitigation strategies are acceptance, avoidance, limitation, and transference.

International Organization for Standardization(2005) states risk treatment strategies to be taken into account as follows:

> Before considering the treatment of a risk, the organization should decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization. Such decisions should be recorded.
>
> For each of the risks identified following the risk assessment a risk treatment decision needs to be made. Possible options for risk treatment include:
>
> - Applying appropriate controls to reduce the risks;(Limitation)
> - Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;(Acceptance)
> - Avoiding risks by not allowing actions that would cause the risks to occur;(Avoidance)

- Transferring the associated risks to other parties, e.g. insurers or suppliers.(Transference)

For those risks where the risk treatment decision has been to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by a risk assessment. Controls should ensure that risks are reduced to an acceptable level taking into account:

- Requirements and constraints of national and international legislation and regulations;
- Organizational objectives;
- Operational requirements and constraints. (p. 5)

Risk Acceptance Criteria

Regarding development and specification of risk acceptance criteria, International Organization for Standardization(2008) states the following:

Risk acceptance criteria should be developed and specified. Risk acceptance criteria often depend on the organization's policies, goals, objectives and the interests of stakeholders.

An organization should define its own scales for levels of risk acceptance. The following should be considered during development:

- Risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances.
- Risk acceptance criteria may be expressed as the ratio of estimated profit(or other business benefit) to the estimated risk
- Different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in non-compliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement
- Risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level with in a defined time period

Risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity. Risk acceptance criteria should be set up considering the following:

- Business criteria
- Legal and regulatory aspects
- Operations
- Technology
- Finance
- Social and humanitarian factors. (p. 8)

Limiting Risks Related to Systems Security Breaches

The basic goal of security is ensuring Confidentiality, Integrity and Availability. These can be ensured through application of encryption, abstraction, layering and data hiding. Security policy development and ensuring newly acquired systems, applications and infrastructures from vendors comply to the companies policy at minimum. Physical security, privacy, authentication, authorization and accounting measures and procedures have to be in place for resources at each layer. Controlling access to databases through the use of appropriate user roles, objects and schemes. Applying operating system hot fixes and patches. Filtering packets using firewalls, IDS and IPS. Putting configuration change management and change management systems to control changes to the production environment. Carrying out regular auditing and penetration tests to identify vulnerabilities

Limiting Risks to Operating System Security

Operating systems have to be hardened during initial installation through patching, by removing unnecessary services, application, and protocols; by configuring users, groups and authentication; by installing additional security controls and finally testing the system security.

Limiting Risks to Applications Security

Applications bridge company's back-end databases/data stores/ and the target consumers of the services the company delivers. Without applications, the static data at the back end is 'life less'. So, applications security is an issue to be taken seriously to mitigate the most possible ranges of attacks that would exploit vulnerabilities in applications.

OWASP Foundation (2013) recommends the following regarding application security configuration tasks:

> In accordance to software installation policy of the company, only install applications that the business environment needs to carry out its missions in order to reduce the number of places vulnerabilities may be found. Carefully select remote access software, if you need any, and properly configure and update it to latest version. All necessary security measures and changes have to be made to applications' default configurations details such as user accounts, passwords and scripting tools. It is also recommended to separate the file access permissions of an account used by applications on servers from accounts that have full permissions on the same server. Application files and directory user access control permissions have to be role based and segmented. In case the application account of the application hosted on the server is compromised by remote attack, this measure will limit its impact.
>
> Securing applications in communication links using public key infrastructure certificates and encryption also prevents traffic tampering and data integrity compromises. For in-house developed applications, follow a strong application architecture that provides effective, secure separation between components. E.g. Some of the compile-time possibilities to mitigate buffer overflow attacks include choosing a high-level language that minimizes vulnerabilities, encouraging safe coding standards and use of safe standard libraries, and including additional code to detect corruption of the stack frame. It is also advisable to run scans and doing audits periodically to help detect future misconfigurations or missing application patches.

Examples of Attack Scenarios

Scenario #1: The application Server admin console is automatically installed and not removed. Default accounts aren't changed. Attacker discovers the standard admin pages are on your server, logs in with default passwords, and takes over.

Scenario #2: Directory listing is not disabled on your server. Attacker discovers she can simply list directories to find any file. Attacker finds and downloads all your compiled Java classes, which she decompiles and reverse engineers to get all your custom code. She then finds a serious access control flaw in your application.

Scenario #3: Application Server configuration allows stack traces to be returned to users, potentially exposing underlying flaws. Attackers love the extra information error messages provide.

Scenario #4: Application Server comes with sample applications that are not removed from your production server. Said sample applications have well known security flaws attackers can use to compromise your server(Top 10 2013-A5-Security Misconfiguration, para. 3-4).

Table 3: Sample application attack vector, security weakness and associated impact

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anonymous external attackers as well as users with their own accounts that may attempt to compromise the system. Also consider insiders wanting to disguise their actions.	Attacker accesses default accounts. Unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system	Security misconfiguration can happen at any level of an application server, database, framework, and custom code. Developers and system administrators need to work together to ensure that the entire stack is configured properly. Automated scanners are useful for detecting missing patches, mis-configurations, use of default accounts, unnecessary services, etc.		The system could be completely compromised without you knowing it. All of your data could be stolen or modified slowly over time. Recovery costs could be expensive	The system could be completely compromised without you knowing it. All your data could be stolen or modified slowly over time. Recovery costs could be expensive.

(OWASP Foundation, 2013, para. 1).

By analyzing and examining six months of web application attacks which included SQL Injection, Remote File Inclusion, Local File Inclusion, Directory Traversal, Cross-Site Scripting, HTTP Violations, Email Extrusion and Comment Spam attack methods ,Imperva revealed that the most prevalent types of attacks are SQL injection, and directory traversal HTTP protocol

violations, which often indicate automated threats, evasion techniques, and denial of service attacks(Imperva, 2013, p. 8).

In addition, Imperva(2013) prescribed the following as measures that organizations should implement to mitigate these attacks:

- Deploy security solutions that prevent automated attacks. To stop automated attacks, security solutions should recognize known automated sources, differentiate between bots and human clients, and detect unusual activity, such as an extremely high rate of Web requests from a single user. Automated attack detection must be identified as early as possible during an attack incident.
- Learn from peers. Applications in similar business verticals may share similar attack characteristics. In the report, they have shown that online retail applications experience about twice as many SQL injection attacks, and fewer RFI attacks than the general application population. Moreover, the SQL injection attacks experienced by online retail applications were much more intensive.
- Detect and block attacks that target known vulnerabilities. The knowledgebase of exploitable weaknesses in an application must be frequently updated.
- Acquire intelligence on malicious sources and apply this intelligence in real time. Black lists of attack sources are still an efficient counter-measure. However, lists must be up-to-date to be effective.
- Participate in a security community and share threat intelligence. The increased automation and scale of attacks leave a large footprint that can only be seen by analyzing data gathered from a large set of potential victims.
- Attack distribution is burst-orientated and far from consistently distributed. Estimations for security measures should be based on the worst case scenario, not on the average case.
- Security procedures and solutions should be as automated as possible, since attack volume is too overwhelming for humans to monitor, and typically, there will be no advance warning of an attack.(p.15)

Limiting Risks Related to Database Security

Default database configuration settings have to be changed. This could be system IDs, passwords and ports. Identifying and filtering out unnecessary packages that could be security risks to the database system, installing database security patches, identifying and disabling useless and vulnerable services, using role and schema object based database access system, employing security logging and auditing techniques , and considering and incorporating security plans at each phase of the database design(Oracle, n.d., para. 4).

Limiting Risks Related to Mobile Devices Security

In today's business environment, mobility has brought its own security risk in addition to its advantages. At times, employees need to connect to the corporate network using mobile devices to execute tasks remotely while at home or field work. The security consideration has to cross the border of the company to reach these mobile devices that are in the employ's pockets. The following are some of the mobile device security measures to have in place in order to limit the security and data risks associated with their use, according to (James et al., 2015):

- Enabling pin-code , swiping or biometric unlocking
- Encrypting the devices
- Enabling remote wiping to be triggered during security risks
- Not storing business confidential data and private information on mobile devices
- Allowing only company trusted and authorized applications to run or install
- Regularly patching operating system updates
- Using firewall, antivirus and enabling any existing security features
- Not discussing sensitive business calls over phones since call tampering is possible; enabling call encryption feature if available
- Avoiding rooting(Android) and Jail-breaking(IOS) since any running code will have root access
- Lock out feature after a number of authentication trials, which will be cleared by administrator
- Using centralized Asset tracking solutions(Mobile Device Management), to locate the devices in case they are lost.(p. 395-400)

Limiting Risks Related to Physical Access to Facility

Not all who comes in has good intention especially when it comes to sensitive business facilities such as data centers. Various ways of physical access monitoring systems have to be installed at checkpoints and gates. These could be security camera, access systems using pin code, biometrics, magnetic cards and multifactor authentication; security guards, multilevel traps and vaulting.

Limiting Risks Related to Electric Power

The damages caused due to over/under voltage generated from electric power source can be mitigated through power regulators installed at appropriate locations and junction points. Some of the devices that are helpful to overcome this damage include surge protectors, backup generators and uninterruptible power supply(UPS) systems.

Limiting Risks Related to Fire Outbreak

No institution is immune to fire. Until the owners/trustees of these institutions develop plans for dealing with the fire threat, they place the building and its occupants, visitors, and collections at risk. The complexity of these plans may vary from a simple evacuation plan, to a fire prevention program, to a more complex plan that includes passive and automatic fire protection systems. Property damaged by floods can often be dried out and restored. Structural damage from an earthquake might be repaired. Stolen property always has a chance of being recovered. Damage from fire, however, is usually permanent and irreparable and once reduced to ash, can never be restored(Andrew, (n.d.), p.1).

There are different classes of fire suppression systems such as Class A, B, C and D depending on the facility being protected. Fire detectors detect fire through smoke, heat, light, sound or combinations of these. Using suppression systems that pump water is not recommended for data center facilities since water seriously damages electronic devices.

- Appoint trained emergency response team to minimize its impact on infrastructure in case fire breaks out.

- Ensure readiness of employee exit.
- Install fire proof walls and closets depending on your budget at hand.
- You need to have lightening protection and grounding systems.
- You can use sprinkler system (that pump water) in areas containing equipments not damaged by water.
- Make sure that electrical circuit wirings are correct and undertaken by a professional to prevent the risk of fire outburst.
- Install appropriate fire alarm systems and performing regular drill tests
- preventing entry of flammable objects into the facility,

The most common types of smoke detectors available and used in buildings today are spottypehotoelectric or ionization. Without going into detail as to their principles of operation, photoelectric detectors react more quickly to smoldering fires that produce visible smoke, whereas ionization detectors react more quickly to invisible products of combustion and flaming fires. The type of detector(s) selected for use may vary from room to room depending upon the construction, furnishings and operations encountered. A fire protection specialist should be consulted for advice. A single spot-type smoke detector can generally protect a room up to 900 square feet. If a room is larger than that, or you want more optimal detection, consider using a mix of photoelectric and ionization detectors in the space.

Smoke detection systems have become rather sophisticated with the advances in computer technology. Today's systems can often list/adjust the sensitivity setting of the detector, adjust for dirty conditions, provide an exact address of the detector [e.g. "Green Room - Second Floor"], and perform specific actions upon activation [e.g. close doors, shut down power, etc.], among other things. Wireless systems are also available, which can be a benefit in historic structures where running wiring may be difficult.

Perhaps the most sensitive smoke detection systems available are the air sampling systems that continually draw and examine the air from a room or rooms. These types of smoke detection are very expensive, and do not readily lend themselves to protecting an entire building. They do, however, offer an aesthetic advantage, in that no visible devices need be installed in the area(s) being protected. Instead, a very small diameter tubing can be discreetly inserted into the room, with nothing visible showing.

Prior to installing a fire detection system, a decision has to be made as to what purpose it's to serve. If the fire detection system is strictly for life safety (the building can burn down as long as everyone gets out in time), then the system need only to sound an alarm in the protected premises. If, however, the intent of the system is to not only sound a local alarm, but also summon trained personnel to fight the fire, then the system must be monitored around the clock. This should preferably be done at the local fire department or a certified control station. Two critical components for ensuring that a fire detection system functions properly are periodic testing and maintenance. Before selecting a system, inquire about service contracts, and check references. It is also very important to protect smoke detectors during operations that produce dust, smoke or spray (e.g., cutting wood, spray painting, welding, burning, etc.). Spray or dust can accumulate on the inside of the detectors rendering them inoperative or causing false alarms. Ensure protective covers are removed and the system is operating when work has been completed for the day. Never leave a detector or system out of service overnight without providing additional fire watches(Andrew, (n.d.), p.7).

Limiting Risks Related to Flood

Floods are one of the major causes of destruction and economic loss in the world. The following are some flood risk limitation strategies:

- Study the flooding/tsunami history on the area and install facilities above its predicted inundation level. It is not recommended to build critical equipments of data centers in basements, where flooding/tsunami is frequent
- Install flood detector and alarm systems in your facility

Limiting Risks Related to Earthquakes

The following are some of the recommended tasks to reduce the effect of disruption caused by earthquakes:

- Construction of buildings has to comply to standardized codes
- Placing rubber bearings into buildings to reduce the impact of seismic waves

- Reinforcing concrete infill walls.
- Strengthening buildings with carbon fibre reinforced polymers. This alternative which can be applied with minimal disturbance to the occupants of a building, is quick and cheap to implement but strong enough to withstand significant earthquake forces.
- Using seismic hazard maps to help urban planners decide what type of building can be built where. They are also used by insurance companies for risk assessments and by civil engineers to assess the magnitude of the earthquake-induced forces to help them design earthquake resistant structures. They help local authorities responsible for emergency management to design plans that can effectively prevent losses and save lives and property (North Atlantic Treaty Organization, n.d., p. 7).

2.5 Alternate Processing Sites

An organization can plan on one of the following most common alternate processing sites that can assume the task of the primary operating site in case of disasters. These are Cold Standby, Warm Standby, Hot Standby and Reciprocal Facility each of which is described below.

Cold Standby

This contains appropriately configured backup resources that are located in remote location. Hardware and software components, network access, and data restoration procedures are implemented manually as needed. This mode requires restarting applications on the backup site as well as enabling network redirection to the new data center. As a result, there may be substantial delay to evolve from standby mode to full operational capability. Recovery Time Objective(RTO) for this scenario can require up to several weeks and Recovery Point Objective(RPO) could also be quite high.

Warm Standby

For an alternating processing site in warm standby mode, applications at the secondary data center are usually ready to start. Resources and services can then be manually activated. It also

provides better RTO and RPO than cold standby but does not provide the transparent operation and zero disruption required for business continuity.

Hot Standby

In this mode, some applications run actively and there is some traffic processing the service tasks. There exists real-time data replication from primary site to secondary site. RTO is usually measured in minutes and RPO is nearly negligible since data mirrored at the secondary site is exactly the same as in the original/primary site. Hence, zero RPO allows applications and services to restart safely. In Active/Active operational mode, hot standby processing site can also be used to relieve the primary site from a heavy workload (Cisco Systems, 2012).

Reciprocal Facility

A reciprocal facility is a legal arrangement between two parties, in which each pledges to make a portion of its facility available to the other party in the event that the other party experiences a disaster that forces it to abandon its own data center. In today's environment, a reciprocal agreement may or may not include the use of the other organization's systems — it may cover just the floor space and power for your systems in the other organization's data center. Still, a reciprocal agreement can cost much less than the alternative, collocation facilities**(**Peter, 2008, p.151).

2.6 Chapter Summary

In this chapter, literatures relevant to business continuity and IT disaster recovery are reviewed. IT disaster recovery is part of an organization's over all business continuity strategy. It accounts for implementation of risk limitation procedures, mapping mission critical business process to underlying IT systems and services, and recovering the IT systems and services in the event of unprecedented disasters. Its success in turn requires handling the human aspects and allocating necessary resources to attain the overall objective of IT disaster recovery preparedness.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1 Overview

In the following section, the research design employed, the sampling design , study location, data collection procedures, and data analysis methods used will be presented.

3.2 Research Design

The research employs qualitative methods. Qualitative – concerned with a quality of information, qualitative methods attempt to gain an understanding of the underlying reasons and motivations for actions and establish how people interpret their experiences and the world around them. Qualitative methods provide insights into the setting of a problem, generating ideas and/or hypotheses (Nicola & Stuart,2008, p.8). Qualitative research is used to look into phenomena involving qualitative data which could be human experience or belief related to a research topic (Kothari, 2004, p.3)

The most common methods of collecting qualitative data include observation, interview and focus groups.

To minimize refusals, the survey researcher should: (a) increase (and emphasize) the benefits of taking part, (b) reduce (and de-emphasize) the drawbacks, and (c) address legitimate concerns of sample members(Edith, Joop, & Don, n.d., p.48).

Thus in order to obtain cooperation, the respondents are clarified with importance of the research especially on the human aspect of business continuity and DR including job security, the benefits of uninterrupted payroll processing, life insurances and safety of personal deposits in banks.

3.3 Sampling Design

Field states that a sample is “a smaller (but hopefully representative) collection of units from a population used to determine truths about that population”(as cited in Shashikant, 2015, p. 15).

The sampling design used is purposive sampling. A purposive sample is a non-probability sample that is selected based on characteristics of a population and the objective of the study. Purposive sampling is also known as judgmental, selective, or subjective sampling.

The researcher targeted 3 positions and an IT manager in each IT departments of the 18 Ethiopian commercial banks for they are in area of expertise related to the research topic. The 18 IT managers are interviewed to obtain the management perspective of IT disaster recovery. Thus, the sample size is 4*18=72.

3.4 Location where the Study is Conducted

This research was conducted at IT Departments in headquarters of 18 commercial banks of Ethiopia. All of the offices are located in Addis Ababa. The researcher conducted questionnaire distribution to and collection from respondents of target expertise, and face-to-face interviews with IT managers.

3.5 Data Sources

Questionnaires and interviews as primary sources of data are used to conduct this research. Questionnaires were administered to a Network Administrator, a System Administrator and a Database Administrator, and face-to-face interview is conducted with IT department managers in each bank. These positions were selected because they are domain area experts in the development and operations of IT disaster recovery plans.

3.6 Data Collection Technique

Questionnaire and Semi- structured interviews were used as means of data collection methods.

Questionnaire design: questionnaire was designed by analyzing components of industry standard IT disaster recovery best practices, books on the topic((Gregory(2008), Snedaker((2007))and literatures reviewed relevant to the area. The questionnaire consisted of likert item type questions each of which with responses on a scale of 1 to 5 (Strongly Agree(1), Agree(2), Neutral(3), Disagree(4), Strongly Disagree(5)). The main topics covered in the questionnaire include risk and business impact analysis, risk limitation, IT disaster recovery plan and its components, IT services protection, and resilience and data protection and recovery.

3.7 Questionnaire Administration

Questionnaires were distributed at each location by the researcher. The researcher followed-up the respondents on telephone for any ambiguity and difficulty the respondents might face while filling the questionnaires.

3.8 Semi-structured Interviews Administration

Semi-structured interviews were designed to gain insight into the management perspective of IT Disaster recovery in the banks. Face-to-face interview was conducted with the IT managers of the respective banks.

In interview design, first the researcher should target respondents whose expertise is relevant to the research questions. The most important consideration is to identify those persons in the research setting who may have the best information with which to address the study's research questions. Second, the researcher should develop an interview guide (sometimes called an interview protocol). This guide will identify appropriate open ended questions that the researcher will ask each interviewee. These questions are designed to allow the researcher to gain insights into the study's fundamental research questions(Dawson & Bob, 2006, p.39).

3.9 Data Processing and Analysis

Data from questionnaires were coded into variables and entered into IBM SPSS Version 23 in order to get frequency distribution of the responses. Finally, pie chart and bar graphs generated using Microsoft Office Excel 2007 and frequency tables are used to display the results of the analysis

In-depth interview was made in Amharic for the simplicity and smooth communication with the interviewee, with the researcher transcribing it in English. Finally, thematic analysis was used to summarize and report the result.

3.10 Operational Definition of Terms

Business continuity: A state of continued, uninterrupted operation of a business (Bank for International Settlements, 2006).

Business Impact Analysis: Business impact analysis is the process of identifying and measuring (quantitatively and qualitatively) the business impact or loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements, and essential staff and to help shape a business continuity plan (Bank for International Settlements, 2006).

Operational Risk: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (Bank for International Settlements, 2006).

Resilience: The ability of a financial industry participant, financial authority or financial system to absorb the impact of a major operational disruption and continue to maintain critical operations or services (Bank for International Settlements, 2006).

CHAPTER FOUR: DATA ANALYSIS AND RESULTS

4.1. Results of the Study

4.1.1 Socio-demographic characteristics of the respondents

This section presents results of the data collected through questionnaires. Total of 53 questionnaires with response rate of 98.14 % were used for analysis. Majority of the respondents were males with frequency 46(86.8%), with 7(13.2%)females. Their educational status shows that 42(79.2%) hold first degree which accounts for more than two-third of the respondents where as the remaining 11(20.8%) hold masters degree. Their professions are Database Administrator, Network Administrator, System Administrator , Chief Technology Officer, V/P IS and Infrastructure Support with frequencies 15(28.3%),13(24.5%),11(20.8%),1(1.9%), 1(1.9%) and 1(1.9%) respectively . However 11(20.8%) of the respondents did not fill their position titles and hence considered as missing.

Regarding the respondent's years of work experience in their respective banks, almost half of them (26(49.1%)) have working experience of [5-9] years.

Table 4: Socio-demographic characteristics of respondents in Ethiopian commercial banks, 2017. (n=53)

Variable	Frequency	Percentage
Gender		
Male	46	86.8
Female	7	13.2
Educational Level		
First Degree	42	79.2
Masters Degree	11	20.8
Position		
Database Administrator	15	28.3
Network Administrator	13	24.5
System Administrator	11	20.8
Chief Technology Officer	1	1.9
V/P Information Systems	1	1.9
Infrastructure Support	1	1.9
Missing	11	20.8
Experience in yrs		
[0-4]	23	43.4
[5 - 9]	26	49.1
[>10]	4	7.5

4.1.2 Risk and Business Impact Analysis

Forty three (81.1%) respondents revealed that the banks have clearly identified disasters that could impact them, whereas 8(15.1%)are indifferent and 2(3.8%) respondents responded that there were no clearly identified disasters that could impact the banks. Similarly, 46(88.5%) respondents strongly agreed/agreed that the banks have assessed risks to IT services and Infrastructure, where as 4(7.7%) are indifferent and 2(3.8%) respondents disagreed. Conversely, only 24 (47.1%) respondents strongly agreed/agreed that there is disaster risk rating by degree of impact, whereas 21(41.2%) respondents are indifferent and 6(11.8%) disagreed/strongly disagreed. While 52(98.1%) respondents strongly agreed/agreed to the statement 'Location of most important business data is known', only 1(1.9%) disagreed on the statement.

Forty nine(92.4%) respondents strongly agreed/ agreed that Mission critical business applications are clearly identified, 3(5.7%) are indifferent and 1(1.9%) respondent disagreed. 23(43.4%) of the responses strongly agreed/ agreed to the statement 'Mission critical applications have clearly set MTD, RPO and RTO values', 23(43.4%) were neutral and 7(13.2%) disagreed/ strongly disagreed.

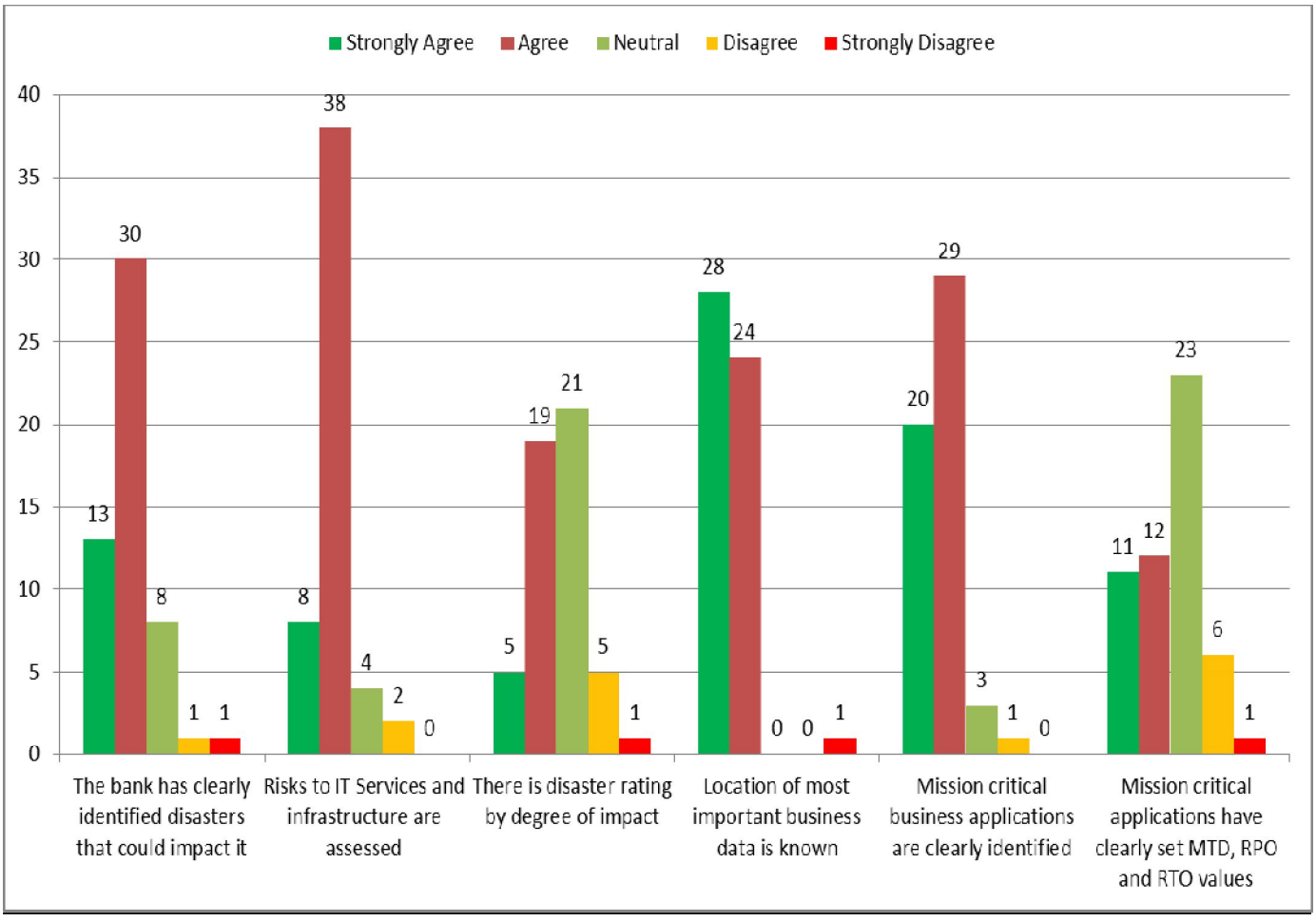
In general 75.23% of the respondents agreed that risk and business impact analysis is performed in the bank they work for.

Table 5: Risk and business impact analysis in Ethiopian commercial banks, 2017. (n=53)

Risk and Business Impact Analysis	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
The bank has clearly identified disasters that could impact it	13 (24.5%)	30 (56.6%)	8 (15.1%)	1 (1.9%)	1 (1.9%)
Risks to IT Services and infrastructure are assessed	8 (15.4%)	38 (73.1%)	4 (7.7%)	2 (3.8%)	0
There is disaster risk rating by	5	19	21	5	1

degree of impact	(9.8%)	(37.3%)	(41.2%)	(9.8%)	(2%)
Location of most important business data is known	28 (52.8%)	24 (45.3%)	0	0	1 (1.9%)
Mission critical business applications are clearly identified	20 (37.7%)	29 (54.7%)	3 (5.7%)	1 (1.9%)	0
Mission critical applications have clearly set MTD, RPO and RTO values	11 (20.8%)	12 (22.6%)	23 (43.4%)	6 (11.3 %)	1 (1.9%)
Total Score	**85 (26.98%)**	**152 (48.25%)**	**59 (18.73%)**	**15 (4.76%)**	**4 (1.27%)**

Figure 7: Risk and business impact analysis in Ethiopian commercial banks, 2017. (n=53)



4.1.3 Risk Limitation

As part of the risk limitation strategy implementation, it is crucial to have centralized authentication system for mission critical application users. 42 respondents strongly agreed/ agreed, 9(17%) are indifferent and 2(3.8%) disagreed to the statement. In addition every application needs some sort of input and output communication to its environment to support the underlying business function it is intended for. Inter-system dependency requirements of mission critical applications have to be identified and documented to minimize the risk of their high downtime. Accordingly 26(50%) respondents Strongly Agreed/ Agreed, 22(42.3%)are neutral and 4(7.7%) disagreed to the statement.36 (67.9%) respondents strongly agreed/ agreed to the statement 'Network addressing, routing and security configuration are documented', 21(39.6%) respondents are indifferent and 1(1.9%) disagreed.

Twenty five 25(48.1%) responses indicate that versions, configurations, patches and fixes for mission critical applications are documented , 21(40.4%) responses being neutral and 6(11.5%) being disagree. Twenty seven (50.9%) respondents strongly agreed/ agreed that they have alternate processing sites, 17(32.1%) respondents being neutral and 9(17%) respondents disagreeing to the statement. The respondents were also asked whether the location of their alternate processing site is not susceptible to disasters. Only eight (15.1%) respondents strongly agreed/agreed that it is not susceptible to disasters, 28(52.8%) respondents were neutral and 17(32.1%) disagreed/ strongly disagreed. Twenty two (42.3%) respondents strongly agreed/agreed to the statement 'the bank has recovery procedures for DNS service, network addressing, routing, boundary defense and voice circuits at alternate processing site', the same number of respondents were also neutral and 8(15.4%) disagreed/strongly disagreed.41(77.4%) respondents agreed to the statement 'The bank has off-site storage for backup media', 6(11.3%) respondents were indifferent and 6(11.3%) respondents disagreed.18(33.9%) respondents strongly agreed/agreed, 23(43.4%) respondents were indifferent and 12(22.6%) disagreed on the statement 'The bank has off-site storage for software and licenses'. Finally, 24(45.2%) responses were in strong agreement/ agreement,18(34%) responses were indifferent and 11(20.8%) responses disagreed to the statement 'I am confident that ways to limit risks to IT Services is implemented .

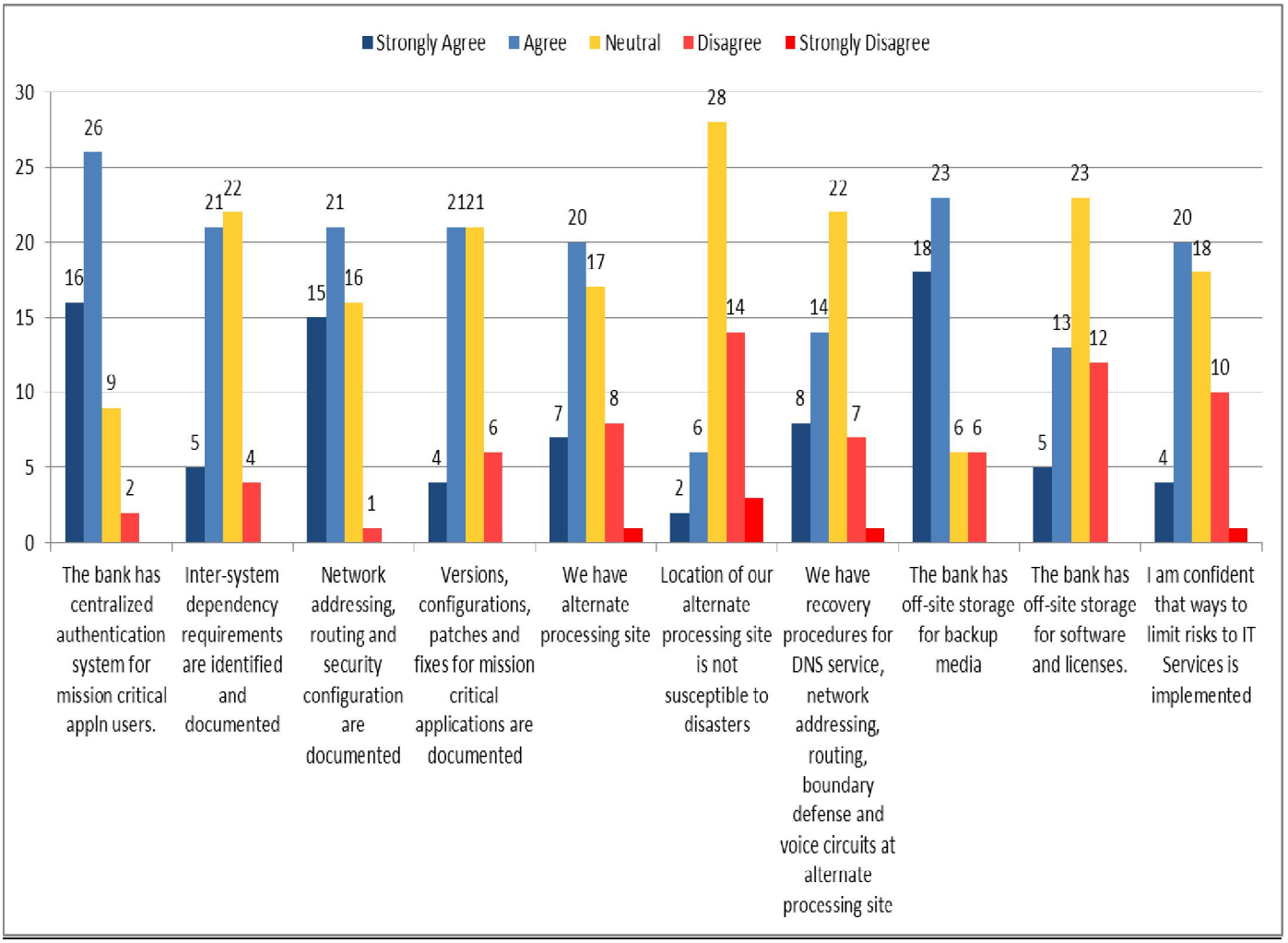
In summary,51.04% of the respondents agreed that Risk Limitation mechanism is in place in the banks.

Table 6: Risk limitation in Ethiopian commercial banks, 2017. (n=53)

Risk Limitation	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The bank has centralized authentication system for mission critical appln users.	16 (30.2%)	26 (49.1%)	9 (17%)	2 (3.8%)	0
Inter-system dependency requirements are identified and documented	5 (9.6%)	21 (40.4%)	22 (42.3%)	4 (7.7%)	0
Network addressing, routing and security configuration are documented	15 (28.3%)	21 (39.6%)	16 (30.2%)	1 (1.9%)	0
Versions, configurations, patches and fixes for mission critical applications are documented	4 (7.7%)	21 (40.4%)	21 (40.4%)	6 (11.5%)	0
We have alternate processing site	7 (13.2%)	20 (37.7%)	17 (32.1%)	8 (15.1%)	1 (1.9%)
Location of our alternate processing site is not susceptible to disasters	2 (3.8%)	6 (11.3%)	28 (52.8%)	14 (26.4%)	3 (5.7%)
We have recovery procedures for DNS service, network addressing, routing, boundary defense and voice circuits at alternate processing site	8 (15.4%)	14 (26.9%)	22 (42.3%)	7 (13.5%)	1 (1.9%)
The bank has off-site storage for backup media	18 (34%)	23 (43.4%)	6 (11.3%)	6 (11.3%)	0

The bank has off-site storage for software and licenses.	5 (9.4%)	13 (24.5%)	23 (43.4%)	12 (22.6%)	0
I am confident that ways to limit risks to IT Services is implemented	4 (7.5%)	20 (37.7%)	18 (34%)	10 (18.9%)	1 (1.9%)
Total Score	**84 (15.94%)**	**185 (35.1%)**	**182 (34.54%)**	**70 (13.28%)**	**6 (1.14%)**

Figure 8: Risk limitation in Ethiopian commercial banks, 2017. (n=53)



4.1.4 IT Disaster Recovery Plan

Thirty two (60.4%) respondents revealed that the banks have IT disaster recovery plan, whereas 11(20.8%) are indifferent and 10(18.9%) respondents disagreed/strongly disagreed. On the other hand, 11(21.5%) respondents strongly agreed/agreed that the banks have disaster declaration procedure, where as30(58.8%) are indifferent and 10(19.6%) respondents disagreed.

14(26.9%) respondents strongly agreed/agreed that the banks have contacts of personnel to communicate during emergency, whereas 23(44.2%) respondents are indifferent and 15(28.8%)disagreed/strongly disagreed. While 14(26.4%) respondents strongly agreed/agreed to the statement 'the bank has emergency response team', 20(37.7%) were neutral and 19(35.9%) disagreed/strongly disagreed to the statement.

Only 7(13.4%) respondents strongly agreed/ agreed that they have emergency leadership selection procedure, 22(42.3%) are indifferent and 23(44.2%) respondents disagreed/strongly disagreed to the statement. Similarly, only 3(5.9%) of the responses strongly agreed/ agreed that the banks have damage assessment teams, 24(47.1%) were neutral and 25(47.1%) strongly disagreed/disagreed.

Nineteen (36.5%) responses indicate that Recovery and restart procedures for vital IT systems are included in their IT Disaster recovery plan, 18(34.6%) responses being neutral and 15(28.8%)being disagree/strongly disagree. Eleven (21.1%) respondents strongly agreed/ agreed that they have IT DR recovery teams responsible for executing system recovery and restart procedures during disasters,17(32.7%) respondents being neutral and 24(46.1%)respondents strongly disagreeing/disagreeing to the statement. The respondents were also asked whether the plan accounts for possible losses of human resources(i.e missing or injured IT workers). Only 7(13.4%) respondents strongly agreed/agreed, 19(36.5%) respondents were neutral and 26(50%)disagreed/ strongly disagreed.7(13.4%) respondents strongly agreed/agreed to the statement 'Contact details of IT DR recovery teams is clearly specified in IT DR Plan', 24(46.2) respondents were neutral and 21(40.3%)disagreed/strongly disagreed. Similarly, only 7(13.4%) respondents agreed that their IT DR Plan contains systems inventories, application inventories, network asset inventories, contracts and service-level

agreements, supplier contact data, and any additional documentation that will aid during recovery, where as26(50%) respondents were indifferent and 19(36.5)respondents strongly agreed/ disagreed.18(35.3%) respondents strongly agreed/agreed, 14(27.5%) respondents were indifferent and 19(37.2%)disagreed to the statement 'should their primary sites go offline, they have procedures for relocating IT operations'.16(30.7%) responses are in strong agreement/ agreement with the statement that they have procedures to transition from alternate processing site to normal operations , 17(32.7%) responses were indifferent and 19(36.5%)responses disagreed/strongly disagreed. On the other hand, 9(17.3%) respondents strongly agreed/agreed that they store IT disaster recovery plan and other crucial recovery documents as off-site storage, where as 20(38.5%) respondents were neutral and 23(44.2%) respondent strongly agree/disagree.

In general only 22.55% of the respondents agreed that their IT disaster recovery plan considers all the 14 statements.

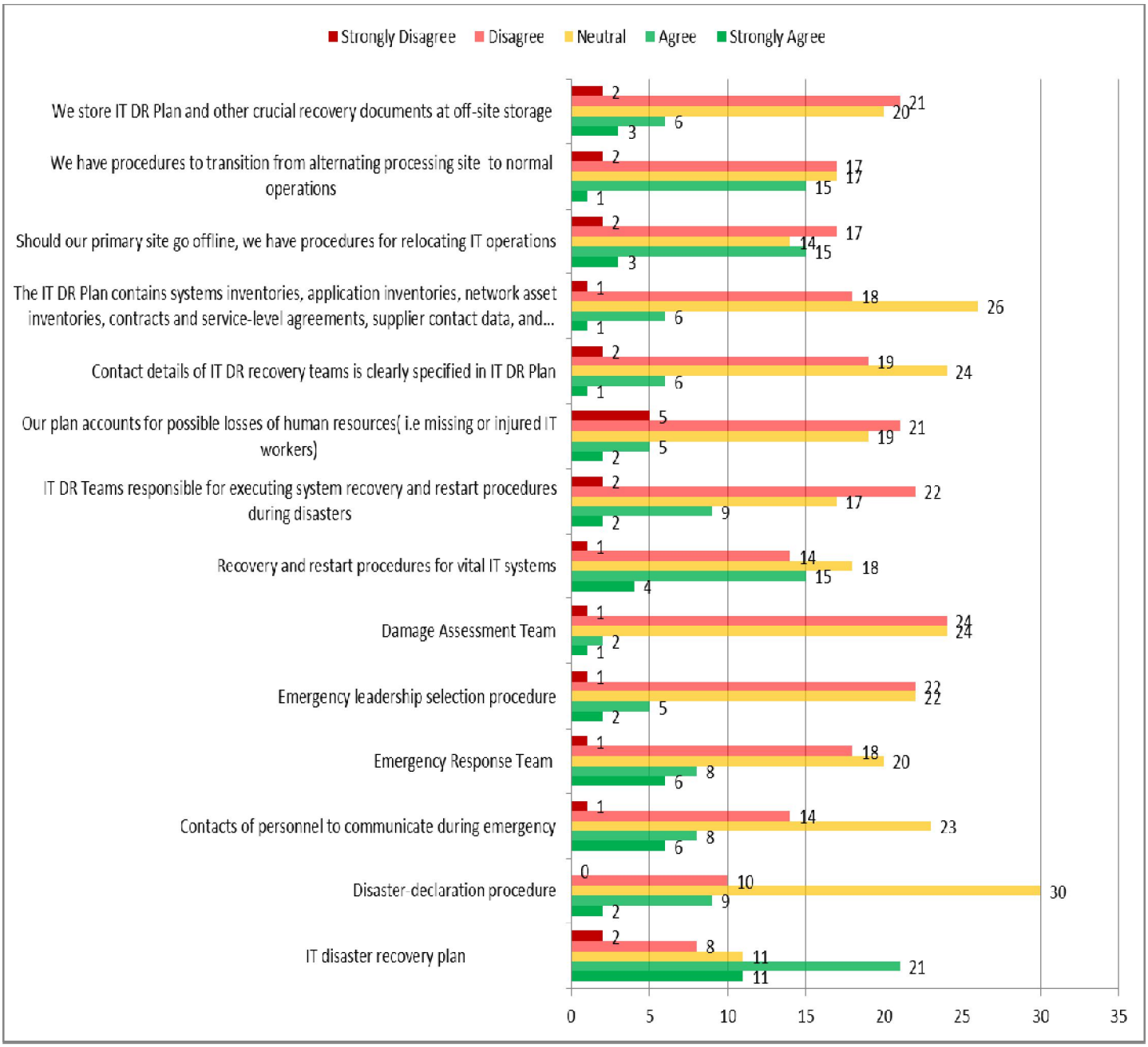
Table 7: IT disaster recovery plan in Ethiopian commercial banks, 2017. (n=53)

IT Disaster Recovery Plan	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The bank has IT disaster recovery plan	11 (20.8%)	21 (39.6%)	11 (20.8%)	8 (15.1%)	2 (3.8%)
Disaster-declaration procedure	2 (3.9%)	9 (17.6%)	30 (58.8%)	10 (19.6%)	0
Contacts of personnel to communicate during emergency	6 (11.5%)	8 (15.4%)	23 (44.2%)	14 (26.9%)	1 (1.9%)
Emergency Response Team	6 (11.3%)	8 (15.1%)	20 (37.7%)	18 (34%)	1 (1.9%)
Emergency leadership selection procedure	2(3.8%)	5 (9.6%)	22 (42.3%)	22 (42.3%)	1 (1.9%)
Damage Assessment Team	1 (2%)	2 (3.9%)	24 (47.1%)	24 (45.1%)	1 (2%)
Recovery and restart procedures	4	15	18	14	1

IT Disaster Recovery Plan	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
for vital IT systems	(7.7%)	(28.8%)	(34.6%)	(26.9%)	(1.9%)
IT DR Teams responsible for executing system recovery and restart procedures during disasters	2 (3.8%)	9 (17.3%)	17 (32.7%)	22 (42.3%)	2 (3.8%)
Our plan accounts for possible losses of human resources(i.e missing or injured IT workers)	2 (3.8%)	5 (9.6%)	19 (36.5%)	21 (40.4%)	5 (9.6%)
Contact details of IT DR recovery teams is clearly specified in IT DR Plan	1 (1.9%)	6 (11.5%)	24 (46.2%)	19 (36.5%)	2 (3.8%)
The IT DR Plan contains systems inventories, application inventories, network asset inventories, contracts and service-level agreements, supplier contact data, and any additional documentation that will aid recovery.	1 (1.9%)	6 (11.5%)	26 (50%)	18 (34.6%)	1 (1.9%)
Should our primary site go offline, we have procedures for relocating IT operations	3 (5.9%)	15 (29.4%)	14 (27.5%)	17 (33.3%)	2 (3.9%)
We have procedures to transition from alternating processing site to normal operations	1 (1.9%)	15 (28.8%)	17 (32.7%)	17 (32.7%)	2 (3.8%)
We store IT DR Plan and other crucial recovery documents at	3 (5.8%)	6 (11.5%)	20 (38.5%)	21 (40.4%)	2 (3.8%)

IT Disaster Recovery Plan	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
off-site storage					
Total Score	**45 (6.3%)**	**116 (16.25%)**	**285 (39.92%)**	**245 (34.31%)**	**23 (3.22%)**

Figure 9: IT disaster recovery plan in Ethiopian commercial banks, 2017. (n=53)



As can be seen from the summarized percent responses shown in figure 10 below,the total percent of disagreement responses is greater than agreement responses for question items B6,C3,C4,C5,C6,C8,C9,C91,C92,C93,C94,C95(refer to Appendix B for the coding of abbreviations). Therefore, the banks need to give attention to address these revealed gaps in their IT disaster recovery practices.

Figure 10: Summarized percent responses of risk and business impact analysis, risk limitation, and IT disaster recovery plan, 2017. (n=53)

	Tagree	Tdisagree	1(Strongly Agree)	2 (Agree)	3 (Neutral)	4 (Disagree)	5 (Strongly Disagree)
C95	17.3%	44.2%	5.8%	11.5%	38.5%	40.4%	3.8%
C94	30.7%	36.5%	1.9%	28.8%	32.7%	32.7%	3.8%
C93	35.3%	37.2%	5.9%	29.4%	27.5%	33.3%	3.9%
C92	13.4%	36.5%	1.9%	11.5%	50.0%	34.6%	1.9%
C91	13.4%	40.3%	1.9%	11.5%	46.2%	36.5%	3.8%
C9	13.4%	50.0%	3.8%	9.6%	36.5%	40.4%	9.6%
C8	21.1%	46.1%	3.8%	17.3%	32.7%	42.3%	3.8%
C7	36.5%	28.8%	7.7%	28.8%	34.6%	26.9%	1.9%
C6	5.5%	47.1%	2.0%	3.9%	47.1%	45.1%	2.0%
C5	13.4%	44.2%	3.8%	9.6%	42.3%	42.3%	1.9%
C4	26.4%	35.9%	11.3%	15.1%	37.7%	34.0%	1.9%
C3	26.9%	28.8%	11.5%	15.4%	44.2%	26.9%	1.9%
C2	21.5%	19.6%	3.9%	17.6%	58.8%	19.6%	0.0%
C1	60.4%	18.9%	20.8%	39.6%	20.8%	15.1%	3.8%
B91	45.2%	20.8%	7.5%	37.7%	34.0%	18.9%	1.9%
B9	33.9%	22.6%	9.4%	24.5%	43.4%	22.6%	0.0%
B8	77.4%	11.3%	34.0%	43.4%	11.3%	11.3%	0.0%
B7	42.3%	15.4%	15.4%	26.9%	42.3%	13.5%	1.9%
B6	15.1%	32.1%	3.8%	11.3%	52.8%	26.4%	5.7%
B5	50.9%	17.0%	13.2%	37.7%	32.1%	15.1%	1.9%
B4	48.1%	11.5%	7.7%	40.4%	40.4%	11.5%	0.0%
B3	67.9%	1.9%	28.3%	39.6%	30.2%	1.9%	0.0%
B2	50.0%	7.7%	9.6%	40.4%	42.3%	7.7%	0.0%
B1	79.3%	3.8%	30.2%	49.1%	17.0%	3.8%	0.0%
A6	43.4%	13.2%	20.8%	22.6%	43.4%	11.3%	1.9%
A5	92.4%	1.9%	37.7%	54.7%	5.7%	1.9%	0.0%
A4	98.1%	1.9%	52.8%	45.3%	0.0%	0.0%	1.9%
A3	47.1%	11.8%	9.8%	37.3%	41.2%	9.8%	2.0%
A2	88.5%	3.8%	15.4%	73.1%	7.7%	3.8%	0.0%
A1	81.1%	3.8%	24.5%	56.6%	15.1%	1.9%	1.9%

Note.

Tagree = percent *Strongly Agree* + percent *Agree*,

Tdisgree =percent *Disagree* + percent *Strongly Disagree*

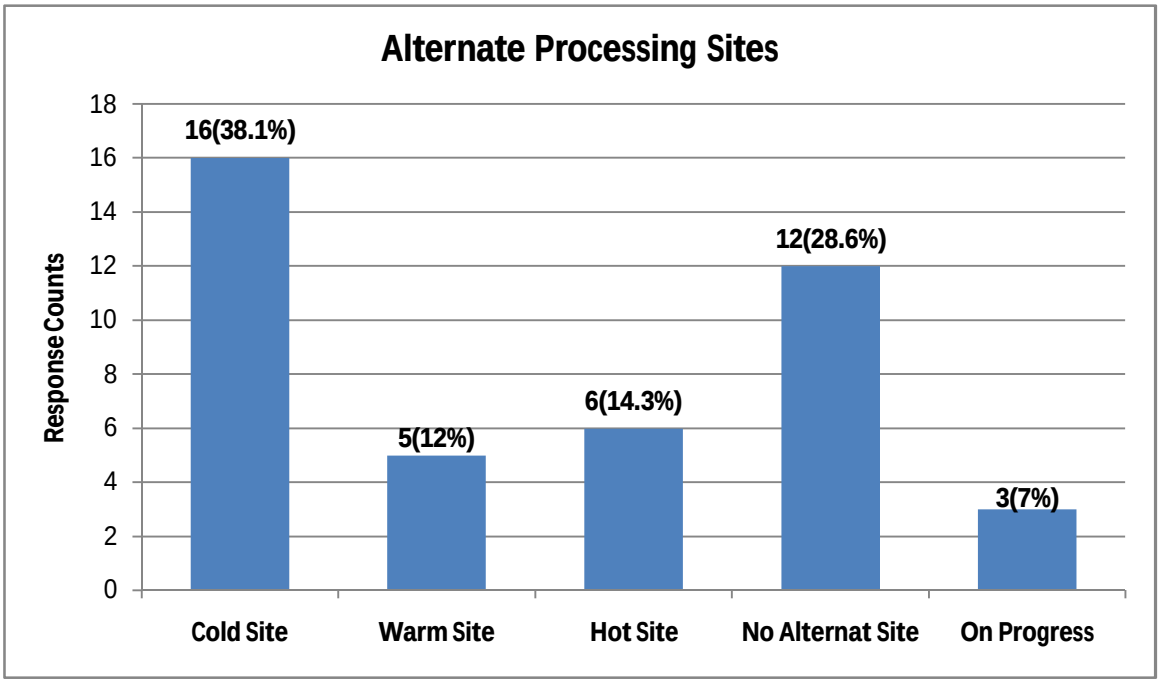
4.1.5 Alternate Processing Site

The chart below shows that 38.1% of the respondents use Cold sites, 14.3% of the respondents use hot sites, 12 % of the respondents use warm site, where as 28.6% of the respondents revealed that they do not have alternate processing sites, and 7% reported that the setup of alternate processing site is in progress. As far as financial institutions such as banks are concerned, having alternate processing site should not be an option. It has to be mandatory to have alternate processing sites to resume operation should the primary site goes down due to unprecedented incident. There has to be strict follow-up and compliance requirement in this regard.

Table 8: Alternate processing sites in Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
Cold site	16	38.10	30.19
Warm Site	5	11.90	9.43
Hot Site	6	14.29	11.32
Reciprocal Site	0	0	0
No Alternate Site	12	28.57	22.64
On Progress	3	7.14	5.66
Total	**42**	**100**	**79.25**

Figure 11: Alternate processing sites in Ethiopian commercial banks, 2017. (n=53)



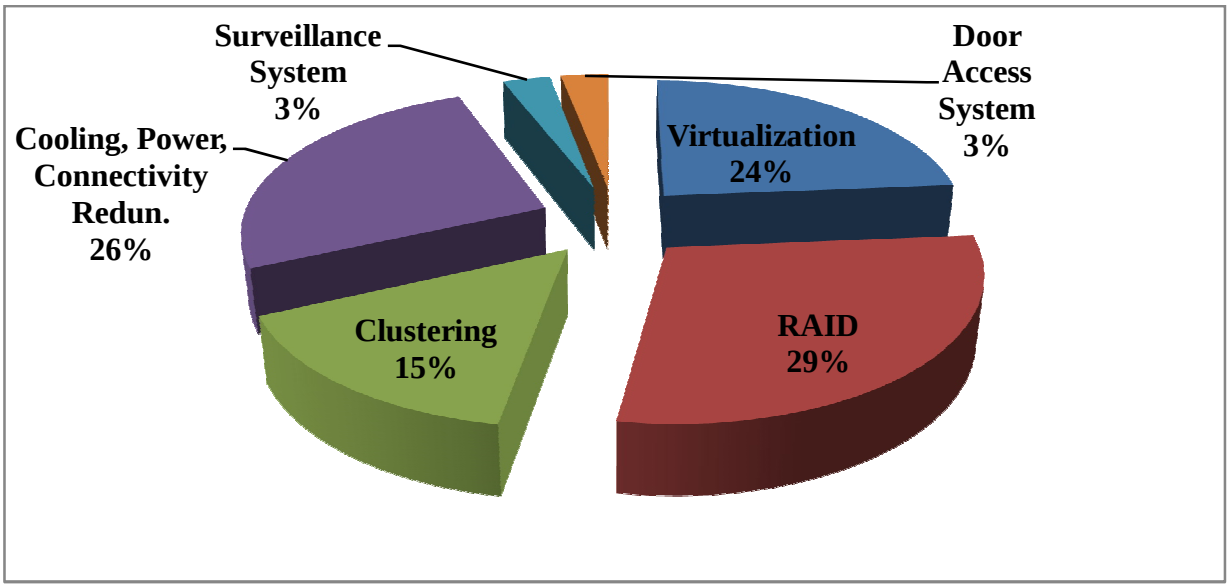
4.1.6 System Protection and Resilience

As can be seen from figure12 below, 28.89% of the respondents have RAID system , 25.93% cooling, power, and connectivity redundancy, 23.7% virtualization technology,15.56% have clustering technology. The additional categories, surveillance and door access systems, reported as system protection and resilience systems by the respondents account for 2.96%. This result shows that the banks have recommended system protection and resilience technologies in place.

Table 9: System protection and resiliencein Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
Virtualization	32	23.7	60.38
RAID	39	28.89	73.58
Clustering	21	15.56	39.62
Cooling, power, connectivity redund	35	25.93	66.04
Surveillance system	4	2.96	7.55
Door Access system	4	2.96	7.55
	135	100	254.72

Figure 12: System protection and resilience in Ethiopian commercial banks, 2017. (n=53)



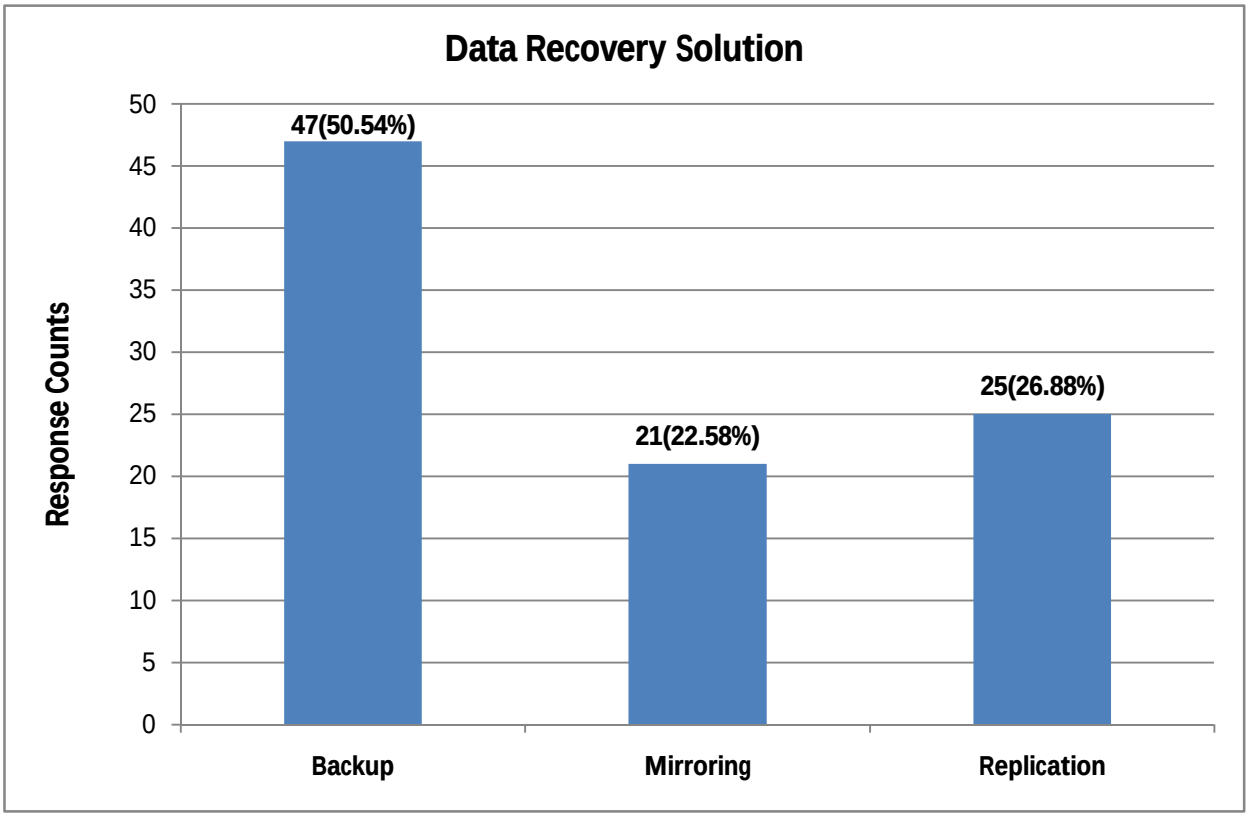
4.1.7 Data Recovery Solution

It can be observed from table below that slightly over half of the responses(50.54%) show backup as data recovery solution, where as 22.58% and 26.88% of the responses indicate the use of mirroring and replication technologies respectively.

Table 10: Data recovery solution in Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
Backup	47	50.54	88.68
Mirroring	21	22.58	39.62
Replication	25	26.88	47.17
	93	100	175.47

Figure 13: Data recovery solution in Ethiopian commercial banks, 2017. (n=53)



4.1.8 Mission Critical Data Backup Frequency

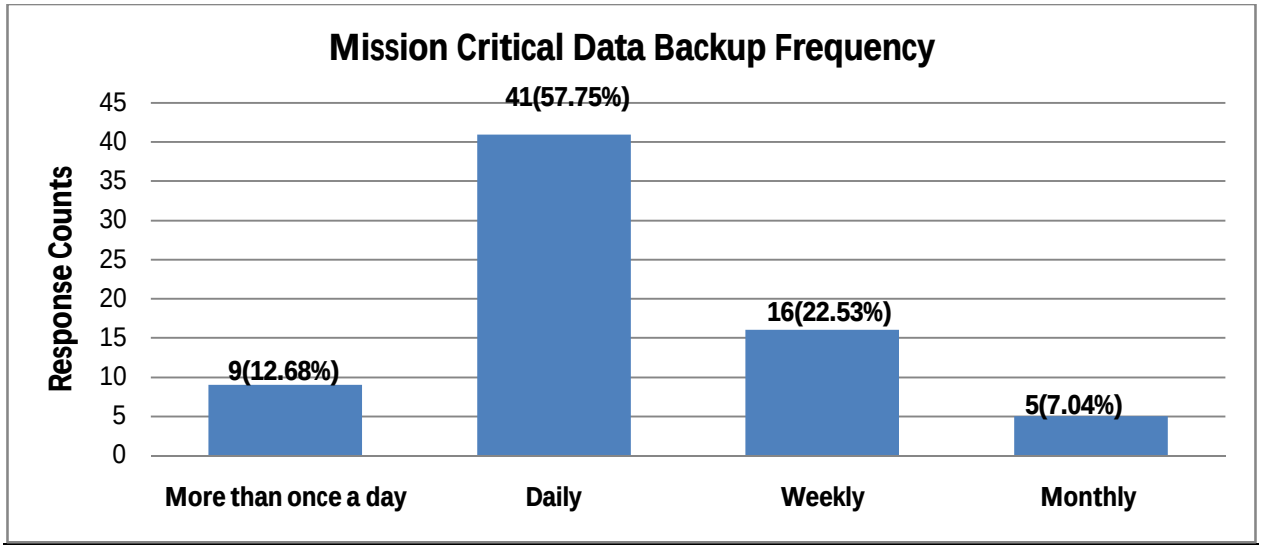
57.75% of all the response counts indicate daily backup, 22.53% of responses indicate weekly backup,12.68% of responses showing backups performed more than once a day, and the remaining 7.04% of total responses monthly backup.

It can be perceived from the result that more than half of the responses with 77.36 % percent of cases indicate the use of daily mission critical data backup in the banks.

Table 11: Mission critical data backup frequency in Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
More than once a day	9	12.68	16.98
Daily	41	57.75	77.36
Weekly	16	22.53	30.19
Monthly	5	7.04	9.43
	71	100	133.96

Figure 14: Mission critical data backup frequency in Ethiopian commercial banks, 2017. (n=53)



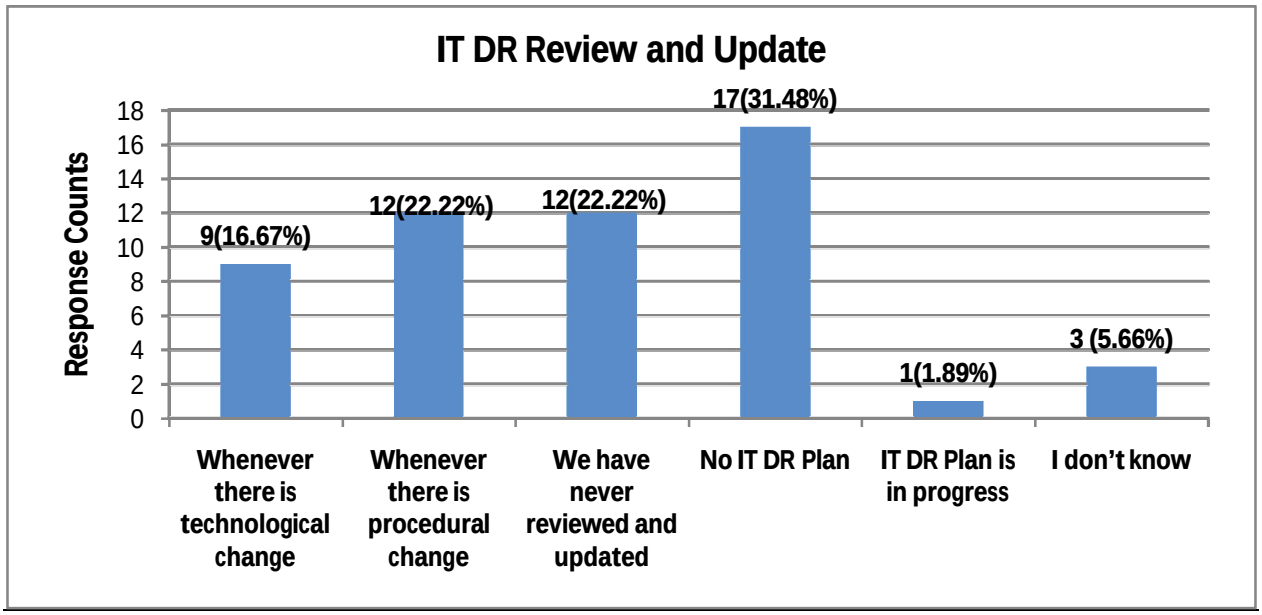
4.1.9IT DRP Review and Update

Twenty two percent of the responses indicate that IT DRP is reviewed and updated whenever there is procedural change. On the other hand, the same number of responses reviled that their IT DRPs have never been reviewed and updated. On the contrary, 16.67% of the total responses reported that the review and update takes place whenever there is technological change. Whereas 31.48% of the responses indicated that they do not have IT DR Plan , 5.56% response showed that they do not know and 1% of the responses showed that their IT DR Plan is in progress. In summary, only 38.89% of total responses revealed that the review and updates take place in response to technological and procedural changes.

Table 12: IT disaster recovery plan review and update in Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
Whenever there is technological change	9	16.67	16.98
Whenever there is procedural change	12	22.22	22.64
We have never reviewed and updated	12	22.22	22.64
No IT DR Plan	17	31.48	32.08
IT DR Plan is in progress	1	1.85	1.89
I don't know	3	5.56	5.66
	54	**100**	101.89

Figure 15: IT disaster recovery plan review and update in Ethiopian commercial banks, 2017. (n=53)



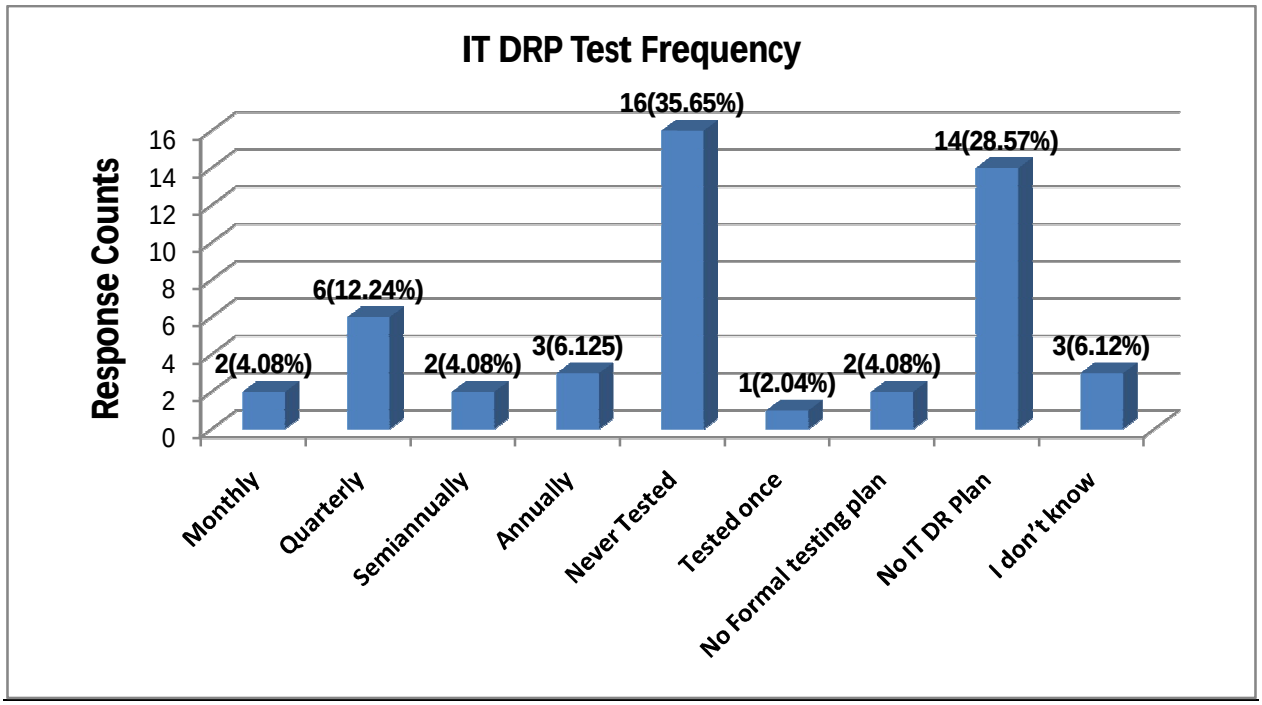
4.1.10IT DRP Test Frequency

28.57 % of the responses specified that they do not have IT DR Plan. 36.73% of the responses indicate that they have no testing frequency plan. 4.08% of the responses show that the test takes place monthly, 12.24% test quarterly, 4.08 % test semiannually, 6.12% test annually, 2.04% tested once, 28.57% have no IT DR Plan and 6.12% do not know. Those that do not have testing frequency plan and no IT DR Plan both sum up to 65.3% which implies that there is unsatisfactory testing practice.

Table 13: IT disaster recovery test frequency in Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
Monthly	2	4.08	3.77
Quarterly	6	12.24	11.32
Semiannually	2	4.08	3.77
Annually	3	6.12	5.66
No testing frequency plan	18	36.73	33.96
Tested once	1	2.04	1.89
No IT DR Plan	14	28.57	26.41
I don't know	3	6.12	5.66
	49	**100**	92.45

Figure 16: IT disaster recovery test frequency in Ethiopian commercial banks, 2017. (n=53)



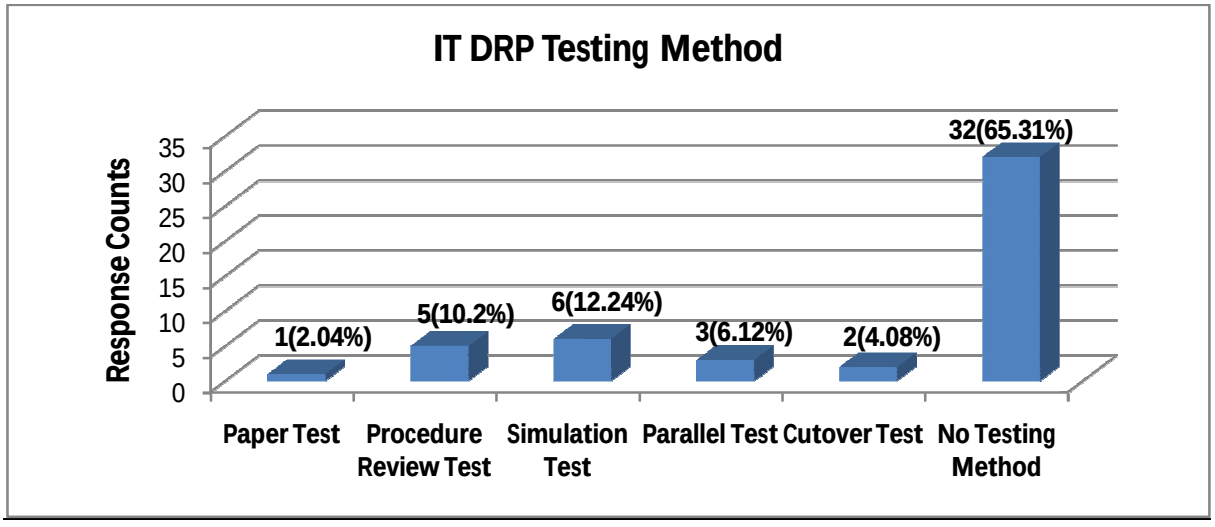
4.1.11IT DRP Testing Method

Percent of the respondents show that 2.04% use paper test, 10.20% use procedure review test, 12.24% use simulation test, 6.12% use parallel test, 4.08% use cutover test where as 65.31% say they have no testing method. As can be seen from the table below, the majority of the respondents (65.31%) revealed that they have no testing method.

Table 14: IT disaster recovery plan testing method in Ethiopian commercial banks, 2017. (n=53)

N=53 Category	Count	Percent of Respondents	Percent of Cases
Paper Test	1	2.04	1.89
Procedure Review Test	5	10.20	9.439
Simulation Test	6	12.24	11.329
Parallel Test	3	6.12	5.669
Cutover Test	2	4.08	3.779
No Testing Method	32	65.31	60.38
	49	100	92.45

Figure 17: IT disaster recovery plan testing method in Ethiopian commercial banks, 2017. (n=53)



4.1.12Results of the Interview

Key participants in this in-depth interview were IT Managers of each commercial bank. The interview questions were tailored to gain the management perspective of IT disaster recovery practices in the banks. The main themes that emerged under each interview points are grouped together and the result is presented as follows:

Alternate processing sites

Only two commercial banks informed that they are using hot alternate processing site.

The following is a statement quoted from one of the two respondents: "*We have hot alternate processing site that operates in Active/Standby mode with the primary site. In case of an incident on the primary site, we manually trigger the standby site to take over the primary operation. The time it takes to bring it up is in minutes*."

The second informant said that they are on a process of constructing a third processing site in Debre-birhan. The location, he said, is selected since it has relatively cold weather condition which reduces the air conditioning expense of the data center. In addition, It would be not so remote for the DR team for the on job fly and support.

This response from one respondent received my attention: "Our headquarter was in bole sub-city area before it moved to its current location. At the time the link between our primary site and alternate site was dark fiber. After we moved our primary site to the new location of our head quarter, we are not able to get the dark fiber service from Ethio-telecom as it ceased providing the dark fiber service to customers. Therefore, even if we have mirroring and replication technologies b/n the primary site and our alternate processing site, we cannot fully exploit their advantage because of recurring link reliability and availability problem b/n our primary and alternate processing site".

Following DRP during emergency situations

One of the respondents said that he remembers an incident in which the virtualization system which hosted some mission critical applications such as internet banking and mobile banking failed. He added that they acted in a reactive manner even though they have some sort of a contingency plan to be followed during such incidents. He added that sharing the contingency plan document, awareness creation and training on the use of the plan was the main gap they noted from the incident.

Five IT managers said that there was no such considerable incident in the past that could require activation of their IT disaster recovery plan.

IT Disaster recovery planning & business strategy

IT disaster recovery plan is considered as part of the overall business risk management strategy. Most of the respondents said that nowadays implementation of IT risk management program is being enforced by national bank of Ethiopia and IT risk compliance assessment team visits them quarterly from the bank. As a result IT disaster recovery planning has got sufficient attention to be considered as part of the business strategy development at the top management.

One respondent said that the bank is considering training and certification programs for their disaster recovery teams. For those with best scores on the raining, he says that the bank is considering to send them abroad and provide them extra training so that they can fully equip themselves with full technical knowledge and expertise required to run the disaster recovery operation.

Three IT managers revealed that IT disaster recovery program has got senior management attention lately and as a result they have prepared tender document and availed it to consultants for execution of the project.

Compliance requirements from National Bank of Ethiopia

- Existence of physical access protection system, fire suppression systems and secure remote access systems in datacenter
- Network boundary defense(firewall, IPS, IDS), domain user management(Password complexity, lockout), traffic encryption and certificate management
- Application user request procedure and existence of user roles as per requirements of business functions
- Establishment of test labs and configuration change managements
- Maximum user that connects to database as sysuser should not exceed 1
- Full database backup retention has to be for 10 years
- The banks are required to have IT disaster recovery plan document and need to stick to it during incidents
- Disaster recovery site has to be tested each 2 months
- Service level agreements (SLA) has to be signed with suppliers for supports.

Considering International standards during development of IT DRP

Two bank managers reported that they are on process of preparing their IT disaster recovery plan with additional objective of constructing a full scale hot alternate processing site. Technical tender document has been prepared and is opened for bidding by competent consultants. One of the components, they say, is compliance to at least a selected international standard which would aid them in quality assurance in case auditing by external parties would be required in the future. The remaining managers said that they will consider incorporating ISO standards.

4.2. Limitations of the Study

This study did not consider factors and challenges that may hold back IT disaster recovery developments in the commercial banks. In addition, the researcher faced limited availability of related literatures in the local context in order to support the study. During the study, two Network Administrators were reported to be on field work and one System Administrator was on leave. Therefore the researcher reached out to staffs with positions Chief Technology Officer, V/P Information Systems and Infrastructure Support to fill out three questionnaires. In addition, 11 respondents did not mention their positions and hence coded as missing. Another factor the researcher noticed as its limitation is that some of the respondents were reluctant to reveal their practices for the fear that the reports of ill preparedness will affect their reputation and images.

4.3 Chapter Summary

In this chapter, results from analysis of questionnaire and interview responses are presented. Frequency tables are used to display the results of commercial bank's risk limitation procedures , risk and business impact analysis, and IT disaster recovery plan and its components. The summarized findings indicate that the banks have performed risk and business impact analysis with significant number of agreement responses where as gaps are observed on risk limitation and IT disaster recovery plan developments and the components considered in the plans.

CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Discussion

The traditional way of having off-site storage sites for storing backups alone would no more make IT disaster recovery feasible. Better high availability and data recovery solutions have to be consumed to minimize the recovery point objectives for essential business applications. This study have investigated IT disaster recovery practices of Ethiopian commercial banks in this regard. The degree to which they have identified at least the high level categories of risks and whether they have analyzed their business impacts in order to prioritize the risks to any identified mission critical applications were assessed.

The extents to which financial institutions prepare for recovery from incidents depend on the context of risk and business profile they operate in. Disasters highly limit access to resources and facilities they might have during normal operations. Therefore, they need to prioritize business applications according to mission criticality by performing business impact analysis(Daniel, 2011). 75.23% of the respondents agreed that risk and business impact analysis is performed in the banks they work for. This shows that majority of the banks have awareness of the risks that could threaten their mission critical IT systems. On the other hand, incase the banks face the risks, they are expected to limit their impacts by having mitigation strategies in place. Accordingly the overall percentage of responses on risk limitation procedures shows that only 51.04% are in agreement. This figure shows that the risk limitation strategy implementation in the banks need full attention. As the world is facing growing number of cyber security threats in addition to natural disasters today, lack of risk mitigation strategy would put the banks in huge vulnerability. Similarly the investigation into their IT disaster recovery plan shows less agreement responses than disagreement on inclusion of contacts of personnel to communicate during emergency , existence of emergency response team, damage assessment team, emergency leadership procedure, IT DR recovery teams and their contacts, off-site storage of IT DRP and related crucial recovery documents as indicated in figure 10 above. This shows that they are responding to incidents in an ad-hoc manner than using a formal recovery plan that considers a modular approach of responding to incidents.

A report from study of IT DR planning practices of 154 banks in the United States shows that even though almost all the banks met main technical elements of IT disaster recovery such as creating backup copies of data and software, acquiring alternative technologies, and developing ways of resuming services, Less than 75% of their IT DR plans addressed human elements of IT disaster recovery planning such as establishing IT disaster response teams, training personnel, disaster notification, establishing communication channels, and formalizing team leader selection procedures during disasters. The study also revealed that technology workers view IT disaster recovery planning as a technical exercise disregarding the level of communication and coordination required in the IT systems recovery process (Christopher & Jordan, 2013).

Finding of an empirical research where data was collected through a questionnaire from IT executives involved in Disaster Recovery from the 11 domestic commercial banks of srilanka shows that the banks are weak in the areas of Disaster Recovery Plan Testing and Maintenance (Fernando, 2008,p. iii).

However the good news is that the percent of agreement is greater than disagreement on whether their IT DRP considers having disaster declaration procedure, and system recovery and restart procedures for vital IT systems.

Regarding the plan testing and test frequency, 65.31% of the responses reported that they have no testing method and 34% of the responses show that there is no testing frequency plan. Plan testing not only helps to verify that the plan works as expected during disasters according to recovery parameters but also helps to identify any skill gap of the recovery team to plan for capacity building through training. Having contingency plan alone is not guarantee for its successful execution during incidents unless the test is undergone through any of the testing methods indicated above. In addition, it has to be noted that as technology and procedures change, plans that are successfully tested today may not be reliable tomorrow unless frequently tested against changing environments(technological/procedural).

64.4% of the responses show that they have alternate processing site, 28% have no alternate processing site and 7% of the responses show that it is on progress. Regarding IT disaster recovery plan review and update, 22% of the responses have never reviewed and updated their plan.

5.2 Conclusion

- Most of the banks performed risk and business impact analysis
- Half of the respondents agreed that risk limitation mechanism is in place.
- IT disaster recovery plans of significant number of the banks did not account for human aspects of IT disaster recovery. In addition, regular plan update and testing are the main gaps observed with significant number of respondents not having any testing method.
- Majority of the banks use cold alternate processing sites.
- Almost half of the responses indicate backup as data recovery solution with the same number of respondents also using daily backup frequency.
- RAID system, cooling, power and connectivity redundancy, and virtualization constitute the top three system protection and resilience solutions the banks
- No bank has considered international standards in its IT disaster recovery development.

This study has shaded light on the current IT disaster recovery practices of Ethiopian commercial banks. It has also identified gaps especially on the human aspects of IT disaster recovery plan, plan update and testing.

5.3 Recommendations

The following are recommendations to the banks and further research areas for future works:

To the banks

- Risks that pose threat to IT systems and services have to be considered as one component of overall risk management with progressive oversight from board of directors.
- Banks have to establish security operation centers to monitor the overall security threats especially at the boundary defense and edge module of the network. Reports of threats that pose risks to IT systems and services have to be provided to the management body on regular basis so that mitigation strategies could be designed in accordance to the changing behaviors of the threats addressed in the reports.
- There have to be information security policies that dictate employees on how to access the banks' data with overall objective of ensuring confidentiality, Integrity and availability of the banks' information systems.
- IT disaster recovery has to be considered as part of the overall business continuity management and disaster recovery teams have to get sufficient training on how to execute their respective responsibilities when disasters hit the primary site. Technological and procedural changes have to be reflected in their IT disaster recovery plans on time and teams have to be established for the follow-up and implementation of these changes according to the banks' change management policies.
- Accessibility of IT disaster recovery plans to all concerned parties have to be ensured by balancing with its confidentiality due to the unpredictable behavior of disasters.
- Dark fiber lease to the banks has to be considered by Ethio-telecom so that they can have autonomous control over the links between their primary sites and disaster recovery sites. In addition, DWDM (Dense Wavelength Division Multiplexing) technology can be considered by the banks to transmit multiple traffic types by altering the wavelengths of the different traffic that pass through the dark fiber.

Further Research Areas

- Further research on development of IT disaster recovery framework tailored to local context of Ethiopian commercial banks
- Research on factors and challenges that may hold back IT disaster recovery developments in Ethiopian commercial banks

References

Brigitte, L., Tim, R.& Mark, S., (n.d).*Disaster Through a Different Lens: A guide for journalists covering disaster risk reduction*. :United Nations International Strategy for Disaster Reduction

Anup, S. (2011, April 06). Japan Earthquake, Tsunami and Nuclear Crisis. Retrieved February 21, 2017, from http://www.globalissues.org/article/794/japan-earthquake-tsunami-nuclear

Aon plc,& Impact Forecasting. (2015). 2015 Annual Global Climate and Catastrophe Report (pp. 1-68, Rep.).

Government of the Union of Myanmar.(2015). *Myanmar Post-disaster Needs Assessment of Floodsand Landslides* (pp. 1-302, Rep. No. 103631).Government of the Union of Myanmar.

Francis, G., & Olivier, M. (September 2010). *Financial Protection of the State against Natural Disasters A Primer* (pp. 1-26, Tech. No. WPS5429). The World Bank

Eduardo, C., &Noy, I. (2010). *The Economics of Natural Disasters A Survey* (pp. 1-49, Tech. No.WP-124). Inter-American Development Bank.

National Bank of Ethiopia.(2012). History of Banking. Retrieved May 18, 2017, from www.nbe.gov.et/aboutus/index.html

New York City Partnership and Chamber of Commerce.(2001). *Economic Impact Analysis of the September 11th Attack on New York City* (pp. 1-151, Rep.). New York

Thomas, V. (2009).*September 11, 2001: Lessons Learned for Planning Disaster Recovery* (Research work, Pace University) (pp. 1-6). New York.

Daniel, A. K. (2011). *Business Continuity for Financial Institutions a Case Study of SG-SSB Limited* (Master's thesis, Kwame Nkrumah University of Science and Technology, 2011) (pp. 1-97). Kumasi.

Bank for International Settlements.(2006). High Level Principles for Business Continuity. Basel Committee on Banking Supervision.

Marianne, S., Pauline, B., Amy, P. W., Dean, G., & David, L. (2010).*Contingency Planning Guide for Federal Information Systems* (pp. 1-149) (USA, U.S. Department of Commerce, National Institute of Standards and Technology(NIST)). NIST.

Gerard, B. (n.d.). *Disaster Recovery 100 Success Secrets: IT Business Continuity, Disaster Recovery Planning and Services*. Aspley, Australia: Emereo Publishing.

Business Continuity Planning.(n.d.). Retrieved from http://www.disasterrecovery.org/

Klaus, S. (2006). *High Availability and Disaster Recovery Concepts, Design, Implementation*. Berlin: Springer.

James, S. M., Mike, C., &Darril, G. (2015).*Certified Information Systems Security Professional Official Study Guide* (7th ed.). Sybex.

Eric, M., & William, S. (2002). *Security Planning & Disaster Recovery*. Berkeley, California: McGraw-Hill.

Bank Supervision Directorate.(2010). *Bank Risk Management Guidelines* (pp. 1-45, Publication). Addis Ababa: National Bank of Ethiopia.

Mogamat, S. F. (2012). *An investigation into Business Continuity Plan (BCP) Failure during a Disaster Event* (master's thesis).University of the Western Cape.

Fernando, A. (2008). *Readiness of Srilankan Banks in Terms of IT Disaster Recovery* (master's thesis).University of Moratuwa.

OWASP Foundation. (2013, June 23). Top 10 2013-A5-Security Misconfiguration. Retrieved from https://www.owasp.org/index.php/Top_10_2013-A5-Security_Misconfiguration

Imperva.(2013). *Imperva Web Application Attack Report* (4th ed., pp. 1-17, Rep.).Imperva.

Vunganai et al. (n.d.).Seismic Hazard Assessment in Eastern and Southern Africa. Retrieved January 13, 2017, from http://www.seismo.ethz.ch/static/gshap/earift/report.html

Susan, S. (2007). *Business Continuity and Disaster Recovery for IT Professionals*. Burlington, MA: Syngress.

Opinion Matters Inc. (2016). The State of IT Disaster Recovery amongst UK Businesses (pp. 1-6, Survey Report). London: Iland.

ACE et. al. (2015). *2015 Data Breach Investigations Report*(pp. 1-70, Rep.). Amsterdam: Verizon Enterprise Solutions.

National Bank of Ethiopia.(2014/2015). *2014/15 Annual Report* (pp. 1-115, Rep.). Addis Ababa: National Bank of Ethiopia.

Kassie, A. (2014). Assessment of the Performance of Ethiopian Financial and Economic Environment. *Global Journal of Management and Business Research*: C Finance, 14(2), 1-7.

Kinde, S. (2002, March). Earthquake Risks in Addis Ababa and other Major Ethiopian Cities - Will the Country be Caught Off-guarded? Retrieved from www.mediaethiopia.com/Engineering/EarthquakeHazard_ET.htm

Diriba, S. (2015).Modeling and Analysis of Ethiopian Banking Sector Performance using BSC and AHP Approaches. *International Journal of African and Asian Studies*, 10,1-12. Retrievedfrom http://www.iiste.org/Journals/index.php/JAAS/article/view/23222

Malssen, K. V. (2006). *Disaster Planning and Recovery: Post-Katrina Lessons for Mixed Media Collections* (master's thesis). New York University.

Cisco Systems.(2008). Disaster Recovery: Best Practices (Publication No. C11-453495-00 02/08).U.S.A.

Bank for International Settlements. (2016, December 30). About the Basel Committee. Retrieved from https://www.bis.org/bcbs/about.htm?m=3%7C14%7C573

International Organization for Standardization.(2008).*Information Technology-Security Techniques-Information Security Risk Management*(ISO/IEC 27005)

Prapawadee, R. N., &Wariya, P. (2009).*Critical Success Factors for effective risk management procedures in financial industries A study from the perspectives of the financial institutions in Thailand* (Unpublished master's thesis). Umeå University.

International Organization for Standardization.(2005).*Information technology — Security techniques — Code of practice for information security management* (ISO/IEC FDIS 17799)

Peter, G. (2008). *IT Disaster Recovery Planning For Dummies*. Hoboken: Wiley Publishing, Inc.

Oracle.(n.d.).*Oracle Security Design and Hardening Support* [Customer Support].

Brenda, P. D. (2009). *Disaster Recovery. Boca Raton*, Florida: CRC Press.

Andrew, W. J. (n.d.). *Assessing Fire Risks and Steps Toward Mitigation* (pp. 1-10) (Smithsonian Institution, Fire Protection and Safety).

North Atlantic Treaty Organization.(n.d.). Earthquake-induced disasters: limiting the damage. Retrieved May 21, 2017, from http://www.nato.int/science/publication/pdf/earthquake-e.pdf

Cisco Systems. (2012). Distributed Virtual Data Center for Enterprise and Service Provider Cloud. Retrieved from http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xr-software/white_paper_c11-694882.html

Nicola, H., & Stuart, M. (2008).*Research Methods Handbook Introductory guide to research methods for social research*. Manchester: Centre for Local Economic Strategies.

Kothari. (2004). *Research Methodology Methods and Techniques* (2nd edition ed.). New Delhi: New Age International (P) Ltd.,

Edith, L., Joop, H. J., & Don, D. A. (Eds.).(n.d.).*International Handbook of Survey Methodology*.

Dawson, H., & Bob, A. (2006).*Doing Case Study Research.* New York: Teachers College Press.

Shashikant, S. N. (Ed.). (2015). *New Perspectives in Sociology & Allied Fields* (1st ed.). EduPedia Publications.

Gerard, B. (n.d.). *Disaster Recovery 100 Success Secrets: IT Business Continuity, Disaster Recovery Planning and Services*. Aspley, Australia: Emereo Publishing.

UN Office for Disaster Risk Reduction (UNISDR).(2014). Ethiopia Disaster & Risk Profile. Retrieved from http://www.preventionweb.net/countries/eth/data/

2016 State of Disaster Recovery Report (Infographic). (n.d.). Retrieved June 26, 2017, from http://www.zetta.net/resource/state-disaster-recovery-2016

Symantec Corporation. (2012). Disaster Preparedness Survey - Global Findings (pp.1-14, Rep.).

Symantec Corporation. (2012). State of Information - SMB Results 2012 (pp. 1-13, Rep.).

Are UK business disruptions on the rise? (n.d.). Retrieved June 26, 2017, from http://www.continuitycentral.com/news07561.html

Telefonica. (2016). Financial Cyber threats Q3 2016 (pp. 1-60, Rep.). Telefonica.

Gregory, P. H. (2008). IT disaster recovery planning for dummies. Hoboken, NJ: Wiley.

Snedaker, S. (2007). Business continuity and disaster recovery for IT professionals: Increase your companys odds of surviving a major disaster. Burlington, MA: Syngress Publishing.

disaster.(2017). In *oxforddictionaries.com*. Retrieved from https://en.oxforddictionaries.com/definition/disaster

Christopher, K., & Jordan, S. (2013). Best Practices in IT Disaster Recovery Planning Among US Banks. Journal of Internet Banking and Commerce.

Central Intelligence Agency.(2017). Ethiopia.*In the World Factbook*. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/et.html

Cummins, J. D., & Mahul, O. (2009).*Catastrophe Risk Financing in Developing Countries.*

risk.(2017). In *oxforddictionaries.com*. Retrieved from https://en.oxforddictionaries.com/definition/risk

LIST OF APPENDIXES

Appendix A – Information Sheet

Dear Participant,

I invite you to participate in a research study entitled Assessment of IT Disaster Recovery Practices in Ethiopian Commercial Banks. I am currently enrolled in Information Science Program at Addis Ababa University and am in the process of executing my Master's Thesis work. The purpose of the research is to investigate how prepared commercial banks are to recover from unprecedented IT Disasters.

Hence, this questionnaire is designed to gather information related to the research title. The data to be collected through this questionnaire will be used only for academic purpose. Your responses will also be kept confidential and you will not be asked to disclose your identity.

The success of this study largely depends on honest and sincere responses that you make to each question items. Therefore, I kindly request you to provide the required information as much as possible.

Thank you for your cooperation in this important endeavor.

Sincerely,

Appendix B–Self Administered Questionnaire

<u>Part I</u>: Statements in this part are intended to obtain an understanding of IT Disaster Recovery Practice in your bank. Let me know if you Strongly Agree, Agree, neither Agree nor Disagree(neutral), Disagree or Strongly Disagree by encircling your answer to each statement.(See example below)

SA: Strongly Agree A:Agree N:Neutral D:Disagree SD: Strongly Disagree

Example question:

I love my profession: (SA) N D SD

In this case the encircled response indicates Strong Agreement with the statement

	Risk and Business Impact Analysis					
1(A1)	The bank has clearly identified natural and man-made disasters that could impact it	SA	A	N	D	SD
2(A2)	We have assessed risks to IT Services and Infrastructure	SA	A	N	D	SD
3(A3)	There is disaster risk rating by degree of impact	SA	A	N	D	SD
4(A4)	We know where most important business data is located in the bank	SA	A	N	D	SD
5(A5)	The bank has clearly identified mission critical business applications	SA	A	N	D	SD
6(A6)	We have clearly set Maximum Tolerable Down Time(MTD), Recovery Point Objective(RPO) and Recovery Time Objective(RTO) values for mission critical applications	SA	A	N	D	SD
	Risk Limitation					
1(B1)	The bank has centralized authentication system for mission critical application users	SA	A	N	D	SD
2(B2)	NB: Mission critical applications depend on other systems or components in order to run properly. The bank has identified and documented the inter-system dependency requirements for mission critical applications	SA	A	N	D	SD
3(B3)	We have documented network addressing, routing and security	SA	A	N	D	SD

	configuration					
4(B4)	We have documented Version, configuration, patches and fixes of all critical applications	SA	A	N	D	SD
5(B5)	We have alternate processing site	SA	A	N	D	SD
6(B6)	Location of our alternate processing site is not susceptible to both natural and man-made disasters	SA	A	N	D	SD
7(B7)	We have procedures for recovering DNS Services, Network addressing and routing, boundary defense, data and voice circuits at alternate processing site	SA	A	N	D	SD
8(B8)	The bank has off-site storage for backup media	SA	A	N	D	SD
9(B9)	The bank has off-site storage for software and licenses	SA	A	N	D	SD
10(B91)	I am confident that we have implemented ways to limit risks to IT Services and Infrastructure	SA	A	N	D	SD
	IT Disaster Recovery Plan(IT DR Plan)& Its components					
1(C1)	The bank has IT disaster recovery plan	SA	A	N	D	SD
2(C2)	We have disaster-declaration procedure	SA	A	N	D	SD
3(C3)	Our IT DR Plan contains contacts of personnel to communicate during emergency	SA	A	N	D	SD
4(C4)	We have Emergency Response Team	SA	A	N	D	SD
5(C5)	We have Damage Assessment Team	SA	A	N	D	SD
6(C6)	We have Emergency leadership selection procedure	SA	A	N	D	SD
7(C7)	System recovery and restart procedures for vital IT systems(servers, operating systems, applications and underlying network configuration) is included in our IT DR Plan	SA	A	N	D	SD
8(C8)	We have IT DR recovery teams responsible for executing system recovery and restart procedures during disasters	SA	A	N	D	SD
9(C9)	Our plan accounts for possible losses of human resources(i.e missing or injured IT workers)	SA	A	N	D	SD
10(C91)	Contact details of IT DR recovery teams is clearly specified in IT DR Plan	SA	A	N	D	SD
11(C92)	The IT DR Plan contains systems inventories, application inventories, network asset inventories, contracts and service-	SA	A	N	D	SD

	level agreements, supplier contact data, and any additional documentation that will aid recovery.					
12(C93)	should our primary site go offline, we have procedures for relocating IT operations	SA	A	N	D	SD
13(C94)	We have procedures to transition from alternating processing site to normal operations	SA	A	N	D	SD
14(C95)	We store IT DR Plan and other crucial recovery documents at off-site storage	SA	A	N	D	SD

<u>Part II</u>: Below are questions with multiple choice answers. Put 'X' mark in the boxes that apply.

1.Which alternate processing site does your bank rely on for IT disaster recovery?

☐ Cold Site ☐ Warm Site ☐ Hot Site ☐ Reciprocal Facility

☐ No alternate site ☐ Other, please specify_____

2. Which system protection and resilience solution is in use in your IT Facility?

☐ Virtualization Technology ☐ RAID Storage system ☐ Clustering Technology

☐ Cooling, Power and Connectivity Redundancy ☐ Other specify _____

_____

3. Which data recovery solution do you have?

☐ Backup ☐ Mirroring ☐ Replication ☐ Other, specify____

4. How often do you take mission critical data backup?

☐ More than once a day ☐ Daily ☐ Weekly ☐ No backup solution

☐ Other, please specify_____

5. When do you review and update IT Disaster recovery plan?

☐ Whenever there is technological change ☐ We do not have IT DR Plan
☐ Whenever there is procedural change
☐ We have never reviewed and updated it so far
☐ Other, please specify_____ _____

6. How often do you test your IT disaster recovery plan?

☐ Monthly ☐ Quarterly ☐ Semiannually ☐ Annually

☐ Never tested ☐ We do not have IT DR Plan ☐ Other, please specify

7. Which IT disaster recovery plan testing method do you use?

☐ Paper test ☐ Procedure review test ☐ simulation test

☐ Parallel test ☐ Cut over test ☐ We have no Testing Method

<u>Part III</u>: Tell me about yourself. NB: No need of writing your name.

1. What is your Gender? ☐ Male ☐ Female

2. Educational level

☐ Diploma ☐ Bachelor Degree ☐ Master's Degree ☐ Phd & above

2. Position _____

3. Years of your experience in the bank ☐ 0-4 ☐ 5 – 9 ☐ >10

Appendix C - Interview Guide

Interview Items to IT Managers

1. Do you have alternate processing site?

2. If you have IT disaster recovery plan, do you think you would strictly follow the plan during emergency situations? Do you follow the DRP during emergency situations?

3. Is IT Disaster recovery planning taken in to account in the bank's business strategy development

4. What compliance requirements are in place from National Bank of Ethiopia regarding IT disaster recovery.

5. Have you considered any international standard for IT disaster recovery plan development