



ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

**AN INVESTIGATION OF CURRENT STATUS OF IT DISASTER
RECOVERY PLAN IN ETHIOPIAN BANKING SECTOR**

BY
HAYLAY GEREZGIHER REDA

OCTOBER, 2017
ADDIS ABABA, ETHIOPIA



ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

**AN INVESTIGATION OF CURRENT STATUS OF IT DISASTER
RECOVERY PLAN IN ETHIOPIAN BANKING SECTOR**

**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: HAYLAY GEREZGIHER REDA

Advisor: Gashaw Kebede (PhD)

October, 2017

ADDIS ABABA, ETHIOPIA



ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

**AN INVESTIGATION OF CURRENT STATUS OF IT DISASTER
RECOVERY PLAN IN ETHIOPIAN BANKING SECTOR**

By: Haylay Gerezgiher Reda

Name and signature of Members of the Examining Board

Gashaw Kebede (PhD)

Advisor

Signature

Date

Workeshet Lamenew (PhD)

Examiner

Signature

Date

Lemma Lessa (PhD)

Examiner

Signature

Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

I declare that the thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Haylay Gerezgiher Reda

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

Advisor's Signature: _____
Gashaw Kebede (PhD)

ACKNOWLEDGMENTS

First and foremost, I would like to thank to the Almighty God and his mother for their endless blessing and motivation bestowed me throughout all seconds, minutes, hours, days, weeks, months and years since the start of my birth day till this long journey of completing this thesis.

I would like to express my sincere gratitude to my advisor Dr. Gashaw Kebede for his valuable comments and continuous supports in completing this thesis. It would have been impossible without his constructive guidance in all stages of writing and submitting of this thesis. Besides, I am very grateful to Dr. Dereje Teferi and Girmay Abraha (PhD candidate) for assisting me when I was selecting a topic and developing proposal on this research area.

I also extend my gratitude to all IT directors of all the banking sectors in Addis Ababa City for showing me good office, and helping me to get the veracious information about the current status of ITDRP in their respective banks. I'm also thankful to all my family and friends for their encouragement and invaluable support to complete my study.

Haylay Gerezgiher

October, 2017

ABSTRACT

In present time, many financial institutions are quickly introducing Information Technology (IT) with a desire to perform their activity efficiently and satisfy the demands that their respective customers. Banks are of these institutions in Ethiopia, which are relying heavily on expanding and introducing IT services for their customers, especially to perform online money transactions. These initiatives and operational progresses are however being hindered by a number of catastrophic situations (possibly natural and manmade disasters), which are of perilous and even causing damage for huge data loss in the institutions. It is in line with this fact that many researches recommended that banks, as financial institutions using computers to fasten their operations and services, must introduce keenly IT Disaster Recovery Planning (ITDRP) to ensure their services and reduce any possible risks and data mutilation and disruption in computers. However, this concern has been inadequately investigated, as there is no particular research dealt with in this regard across all the banking sectors in Ethiopia. The objective of this study was thus to examine the current status of ITDRP in banking sector located in Addis Ababa City. To this end, the study methodologically used a mixed research design. A total of nineteen respondents were used to respond the questionnaires from the nineteen banks of Ethiopia, which contained both close-ended and open-ended questions. Technically, the respondents were selected through purposive sampling. The quantitative data findings were analyzed through SPSS a computer software program, version 20; whereas, the qualitative findings were through a simple thematic analysis approach. Accordingly, the study found that 42.1% (8) of the banks implemented ITDRP in place; whereas 57.9% (11) of the banks didn't put it to work so far, but they are under progress status. However, 42.1% (8) of banks who have the plan in place are still supposed their plan is not real as it needs major technical improvements to meet its intended purpose. According the findings of this research, the researcher concluded that ITDRP is not exercising well at Ethiopian banks due to less emphasis given to it from the top managers and inexperienced of sever disaster strike heretofore. Even though the study has its own limitation, the findings allow us to provide practical implication, recommendation for the banking sector and directions for future works.

Keywords: Information Technology (IT), Ethiopian banks, IT Disaster Recovery Plan (ITDRP)

Table of Contents

ACKNOWLEDGMENTS	V
ABSTRACT.....	VI
LIST OF TABLES	X
LIST OF FIGURES	XI
LIST OF ACRONYMS	XII
CHAPTER ONE	1
1.1. Back ground of the study	1
1.2. Banking History in Ethiopia	2
1.3. Statement of the problem	3
1.4. Research questions.....	4
1.5. Objectives.....	5
1.5.1. General objective	5
1.5.2. Specific objective.....	5
1.6. Significance of the study.....	5
1.7. Scope and delimitation of the study	6
1.8. Organization of the thesis.....	6
CHAPTER TWO	7
2. LITERATURE REVIEW	7
2.1. Introduction.....	7
2.2. IT Disaster Recovery Plan.....	7
2.2.1. IT Disaster Recovery Plan Components.....	10
2.1.2. IT Disaster Recovery Planning Processes	11

2.3.	IT Disaster Identification	13
2.3.1.	What is a disaster?	13
2.4.	IT Disaster Recovery Plan in Financial Industry	15
2.5.	The Importance of IT disaster recovery plan for Banks.....	16
2.6.	IT Disaster Recovery Strategies	17
2.7.	Tiers of IT Disaster Recovery Plan	18
2.8.	Types of IT Disaster Recovery Techniques	21
2.9.	Selecting ITDRP Testing Methodologies	22
2.10.	Standards and guidelines for IT disaster recovery plan	24
2.11.	Related works	27
2.12.	Chapter summary	32
CHAPTER THREE		33
3.	RESEARCH METHODOLOGY	33
3.1.	Introduction.....	33
3.1.	Research design.....	33
3.3.	Data Collection Methods	35
3.4.	Approaches of data analysis.....	36
3.5.	Research reliability and validity	36
3.6.	Ethical issues consideration	37
CHAPTER FOUR.....		38
DATA PRESENTATION, ANALYSIS & DISCUSSION.....		38
4.	Introduction	38
4.1.	Research and statistical tools employed.....	38

4.2.1. Quantitative Data Analysis from Ethiopian Banks	38
4.2.2. Findings from the Qualitative Data	53
4.2.3. Discussion.....	55
4.2.4. Chapter summary	56
CHAPTER FIVE	57
CONCLUSION AND RECOMMENDATION	57
5. Introduction	57
5.1. Conclusion	57
5.2. Practical implication of the study.....	58
5.4. Limitations and Future works of the study	60
REFERENCES.....	61
APPENDICES	65
Appendix A: Letter of cooperation written by the university to the banks.	65
Appendix B: Survey Questionnaire.....	66
Appendix C: Letter request for cooperation to IT Infrastructure unit at UNITED BANK S.C	72

List of Tables

Table 2.1: The seven IT DRP phases.....	11
Table 2.2: Examples of man-made disasters.....	15
Table 2.3: Alternate site decision criteria	22
Table 2.4: summary of related works	31
Table 3.1: list of target banks of Ethiopia.....	34
Table 4.1: Frequency distribution of the banks category.....	39
Table 4.2: ITDRP * Documentation Cross tabulation.....	42
Table 4.3: Frequency distribution of the banks which incorporated the plan.....	43
Table 4.4: Frequency distribution of the off-site location among the banks	43
Table 4.5: Frequency distribution of ITDRP recovery capability among the banks	46
Table 4.6: Frequency distribution of ITDRP testing among the banks	47
Table 4.7: Type of testing response frequency and percentage distribution.....	48
Table 4.8: ITDRP auditing responses frequency and percentage distribution.....	48
Table 4.9: Type of ITDRP auditing frequency distribution among the banks.....	50
Table 4.10.ITDRP effectiveness frequency distribution among Ethiopian banks.....	51
Table 4.11 ITDRP budget revision frequency distribution among the banks.....	53

List of figures

Figure 2.1: Planned versus unplanned outages for IT operations	8
Figure 2.2: BCM, BCP & DRP Context	9
Figure 2.3: Elements of disaster recovery plans	10
Figure 2.4: Disaster recovery planning phases	11
Figure 2.5: Model of Types of Disasters	14
Figure 2.6: IT Disaster recovery plan phase	17
Figure 2.7: The typical length of time for the recovery in seven tiers.....	21
Figure 2.8: Illustration of an ITDRP Cycle Testing Scenario	24
Figure 2.9: COBIT Principles	25
Figure 2.10: ITIL frame work	26
Figure 4.1: Current Status of ITDRP in Ethiopia banks	41
Figure 4.2: Frequency distribution of ITDRP standards usage in Ethiopian banks.....	45
Figure 4.3: Frequency distribution of ITDRP testing experience among the banks.....	48

LIST OF ACRONYMS

ATM -Automated Teller Machine

BCM - Business continuity management

BCP - Business Continuity Plan

BIA - Business Impact Analysis

COBIT - Common Objective for Information related and Technology

CP - Contingency Planning

DR - Disaster Recovery

FIPS - Federal Information Processing Standards

IBM - International Business Machine

ICT- Information Communication Technology

IEC - International Electrotechnical Commission

IFRC- International Federation of Red Cross and Red Crescent Societies

IMP - Incident Management Plan

IRBC-ICT Readiness for Business Continuity

ISO - International Standard Organization

IT - Information Technology

ITDRP-Information Technology Disaster Recovery Plan

ITIL- Information Technology Infrastructure Library

NBE-National Bank of Ethiopia

NIST -National Institute of Science and Standard

PTAM - Pickup Truck Access Method

RA - Risk Assessment

RBI - Reserve Bank of India

RPO - Recovery Point Objective

RTO - Recovery Time Objective

SP – Special Publication

SPSS – Statistical Package for Social Science

Chapter One

1. Introduction

1.1. Back ground of the study

In this world the swiftly change of computer technologies and dependency on such technologies are increasing the risk of data loss [1]. Now a days stable and reliable IT services have become the minimum required for business organizations [2]. Modern banks and financial institutions cannot perform their functions without the use of Information systems for data processing, storage and communication. Banking sector is the backbone of entire financial economy of the country, because it highly supporting the money transactions and doing business over the past decades.

And banks becomes highly dependent on Information Technology (IT) to enhance business operation, facilitate management decision-making, and deploy business strategies and to reach out new customers [3]. Therefore, IT system availability has become one of the most critical issues that attracted attention from multi directions including, business managers, practitioners and researchers. In specifically, some organizations (financial institutes, high volume online retailers, government departments, utility companies, *etc.*) require that an IT system operates continuously; those organizations cannot tolerate any failure. But at the same time, there are different natural and man-made disasters that cause for concerns of IT based business continuity. Our country Ethiopia is not well experienced by massive natural disaster so far. Nonetheless we haven't to ignore the possible risks of using IT without business continuity plan in place. Because unawareness and ignorance of environment is also leading the increase in risk associated with data storage system. There are different conditions in which banks and other financial institutions may cause system interruption, data loss leading huge business loss and/or dissatisfaction amongst the customers.

Natural and man-made are the most common disasters that can lead to data loss which in turn can cause a billion of dollars of money lost. "The International Federation of Red Cross and Red Crescent Societies (IFRC) found 7184 disasters from 2000 to 2009, ranging from the Bhopal disaster, the tsunami in Indonesia in 2004, hurricane Katrina in 2005, the Haiti earthquake in 2010 and the Chernobyl explosions to the September 11th attack on the World Trade Centre in New York" [4]. There are also other high-profile incidents seen in different countries, such as terrorist attack and civil unrest which could turn in to devastating problems for business organizations.

Despite the enormity of such events, they form only part of an increasingly complex set of factors to be considered as potentially significant threats for many businesses organizations.

Since 9/11 attack of world Trade Center twin towers in New York in the year 2001 most organizations led to consider the importance of adequate Information Technology Disaster Recovery Plan (ITDRP) in place. However, in Ethiopia there are not previous works on ITDRP that indicate how the government and private organizations works on all types of disasters and their counter measures. A disaster is any event that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operations of the business [5].

Business continuity (BC) is vital for any business organizations in order to survive in competitive environment. But it's more critical for organizations that deal with financial transaction and online data storage, where a minute may be worth several billions of dollars. In today's environment almost all banks in Ethiopia are highly depend on computer based system. Therefore, any down time in the banks can cause loss of huge amount of dollars and it could leads to dissatisfaction among the customers. The motivation for this study is because the area is blistering issue across the globe but there are still limited research works so far related to this research topic. Thus, at the outset I motivated to explore the ITDRP current status in Ethiopian banks because of its irreplaceable advantages for financial institutions (banks).

1.2. Banking History in Ethiopia

As history indicated that the modern sense of banking service in Ethiopia was began towards the end of Emperor Minilik II. And the first bank was opened in 1906 E.C with cooperated the British owned National Bank of Egypt and it was called Bank of Abyssinia. At that time the bank was totally managed by the Egyptian National Bank with the specified rights and concessions that were agreed upon the establishment of Bank of Abyssinia and the initial capital was 500,000 pound sterling. However, this time the number of banks in Ethiopia are tremendously increasing from time to time due to economic development of the country and societies as well. Currently there are 16 private and 2 governmental owned banks and one central bank in Ethiopia that transact millions of birr per day [6]. The main functions of banks are to give flexible money transaction services for the customers and organizations continuously, but there are natural and manmade disasters that could prevent the banks from performing their tasks normally. So there is called Business Continuity Plan (BCP), BCP describes the steps an organization takes when it cannot operate

normally because of a natural or manmade disasters [7]. BC and disaster recovery are critical components used to ensure that systems essential to the operation of the organization are available when needed. Since banks are a service provider for individuals, organizations; therefore they should have ITDRP in place in order to rely on by their respective customers. Nowadays banks are come up with highly sophisticated technologies in order to get competitive advantages over their rivalries. But this should not enough for banks to stay in the market for long time, because natural or manmade disasters could disrupt their business process and the whole system for extensive time. So banks need to adopt BCPs and disaster recovery strategies to avoid intentional or unintentional problems that prevent the system from operating its normal business processes. DRP is the counter measure for all disasters that written for a specific business process or may address all mission-critical business processes and IT infrastructures.

1.3. Statement of the problem

Nowadays computerized banking system is highly promoted in Ethiopian banking sector to facilitate customer's daily money transactions and for decision making of top managers, but there are natural and manmade adversities that could halt their business continuity and make the system failed to function normally. Worldwide, businesses continually increase their dependence on IT systems for routine business processes. The business processes which directly rely on information systems and the supporting IT infrastructure often require high levels of availability and recovery in the case of an unplanned outage [8]. As a result, the process of BC must intimately relate business processes to the traditional process of IT disaster recovery. In Ethiopia the number of banks are increasing in the recent times and they are attracting millions of customers because of their flexible electronic money transaction services such as core banking, Automated Teller Machine (ATM) networks, Tele-banking and internet banking. Nonetheless, there are things to be considered by the bank's top manager for their existence in the market and keeping the business alive. Therefore disasters are the major issues to be include in the BCP of the banks. Disaster is defined as a sudden, unplanned catastrophic event that renders the organizations ability to perform mission-critical and critical processes, including the ability to do normal production processing of systems that support critical business processes. Business interruptions can occur anywhere, anytime due to massive hurricanes, tsunamis, power outages, terrorist bombings etc. [9]. In today's world it has become mandatory to prepare for such disaster scenarios always. IT disaster identification and notification, is based on the procedures which have been developed for detecting

IT disasters, for communicating during emergencies, and for warning IT disaster recovery team members and other stakeholders [10].ITDRP is interrupted availability IT resources that support key business operations of an business organization. ITDRP has gained significant momentum in last few year, especially with the increasing of corporate dependence on computer systems and the growing levels of desolation associated with the recent adversities [9] [10]. Presently this research topic is hot issue across the globe but it still receive little attention from researchers. The advance of banking sector have brought in an era multi-product and multi-service being delivered using multiple yet integrated channels [9]. The rising competition and customer expectations have compelled the top management to implement, and continuously upgrade, agile and scalable IT practice and solutions for their banks. The use of information and communication technology (ICT) is on increasing and encompasses nearly the entire gamut of banking operations and services. Nowadays in Ethiopia all the banks are highly depend on ICT to facilitate the main functions/services and to reach out their customers across the country as well the globe. However, the world has experienced different unwanted situations like the recent massive natural disasters in japan and Nepal. The disruption of financial institution including banks can occur anywhere at any time and it is not possible predict what may strike like earth quick, tsunami, civil unrest and power outages, etc. Banks in Ethiopia are not well experienced by sever natural or human made disaster disruption but there are some service interruptions because of power outages and frequent breakage of data communication service from telecommunication service provider. Hence, it has become very important for financial institutions to have ITDRP in place to avoid any potential loss data. Otherwise the lack of having BC could affect the continuous operation of the mission critical services.

1.4. Research questions

Based on the statement of the problem described above, the study is aims to answer the following research questions:-

- ❖ To what extent ITDRP is practicing in Ethiopian banks?
- ❖ How often does each Ethiopian bank test, review, and audited their ITDRPs?
- ❖ Do the banks have properly placed an alternative site?

1.5. Objectives

1.5.1. General objective

The general objective of the study is to examine the current status of IT Disaster Recovery Plan in Ethiopian banking industry.

1.5.2. Specific objective

The following specific tasks will be carried out in order to complete the above general objective:-

- ✓ To review different literatures related to IT disaster recovery plans
- ✓ To identify whether each bank has a IT disaster recovery plan in place
- ✓ To identify how often plans are tested, reviewed and updated
- ✓ To assess if plans are incorporated in corporate strategies
- ✓ To identify the bank's IT DRP standards
- ✓ To explain how often plan are audited
- ✓ To make an appropriate recommendation how to design adequate and effective ITDRP for Ethiopian banks based on the best international standards and practices

1.6. Significance of the study

Today ITDRP is not an option for business organization but it is must. Because IT disaster recovery plan is one of the main aspects of BCP that always need to adopt; continuous testing and modify according the natural and human factor by the business organizations in order to resume to normal operation in considerable time after and during disaster attacks. As the purpose of the study is to assess the current ITDRP status and experience of Ethiopian banks regarding of the possible environmental risk factors. As consequence the researcher would come up with recommendations of the best practices, procedures and strategies to be used for ITDRP by the local banks in according the literatures and best world practices. As a result, IT practitioners could use it for designing ITDRP for their business organizations and academicians could take as bench mark for the next research works. The following are some of the important points that the banks can take out from this study:

- ✓ They can help them to reassess the environmental risk factors, business impact analysis and deploy comprehensive ITDRP for their organization.
- ✓ To improve the general understanding of top managers on the importance of having ITDRP and BCP in place

- ✓ To harmonizes the traditional concepts of ITDRP with the modern practices and international custom of ITDRP
- ✓ IT professionals of the banks can have better insight towards the ITDRP deployment
- ✓ Researchers could take it as benchmarks for further study

1.7. Scope and delimitation of the study

The study was mainly focused on assessing the current ITDRP status in Ethiopian banking sector. In this study the researcher assessed the DR strategies, procedures, testing, reviewing and auditing policies of the banks in Ethiopia. Totally Nineteen banks two governmental, one from NBE and sixteen private owned banks were directly involved for purpose of the study. But the study was not covered the other financial institutions due to time and resource limitations.

1.8. Organization of the thesis

This thesis has organized in five chapters. The first chapter contains the background of the study, problem statement, objectives, scope, and significance of the study. The second chapter deals about literature review related to ITDRP components, ITDRP breakthrough at financial institutions, ITDRP recovery strategies, ITDRP implementation standards, ITDRP testing policies and challenges of implementing ITDRP. The third chapter contains about research design, target population, data collection instruments, instrument reliability and validity and ethical issues needed to be consider. The fourth chapter is about data presentation, analysis and discussion of the results found from both quantitative and qualitative data. The last chapter presents the conclusion, recommendation and directions for further study conferring the research findings.

Chapter Two

2. Literature Review

2.1. Introduction

This chapter reviews different literatures that are related to the objective of the study. The literatures covered under this section deals about the general concept and definitions of ITDRP, BCP, and the anticipated types of disaster. Literatures also discussed on the components of ITDRP, evolution of ITDRP in financial institutions, ITDRP strategies, ITDRP testing policies and about the different tiers of disaster recovery with related to their cost effective and recovery time capability. In addition to the above points, this section discussed about the importance ITDRP for financial institutions including banks and the challenges of banks in deploying ITDRP for their mission critical business operations.

2.2. IT Disaster Recovery Plan

Since September 11, 2001 terrorist attack in United State business organization are focusing on attention of organization decision makers on the urgent need to prepare for disaster recovery [7].According [11] BCP is the broad process that involves the recovery, resumption, and maintenance of the entire business, not just the technology component. BCP is a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events [12].Business Continuity Management (BCM) is the development of strategies, plans, and actions to protect or provide an alternative mode of operations for business processes that, if interrupted, could seriously damage or cause fatal losses to an organization [13]. BCM includes BCP, DRP and crisis management. DRP which is often used interchangeable with BCP is one of the core points of BCM recovery that deals with rebuilding and recovery after disaster. BCM or planning is the development, implementation and maintenance of policies, frameworks and programs to assist treasury manage a business disruption, as well as build treasury resilience [14].

BCP is an enterprise wide planning process which creates detailed procedures to be used in the case of a large unplanned outage or disaster. Maintaining continuity of business processes is the overall objective [15].From an IT-centric perspective, outages are classified as planned or unplanned disruptions to operations. An unplanned IT outage can equate to a disaster, depending

on the scope and severity of the problem. Many Disaster Recovery plans focus solely on risks within the data center. But disaster recovery plans should cover all the business mission-critical tasks and the information system as whole. The following figure shows the common types outages widely experienced in enterprise computing environments.

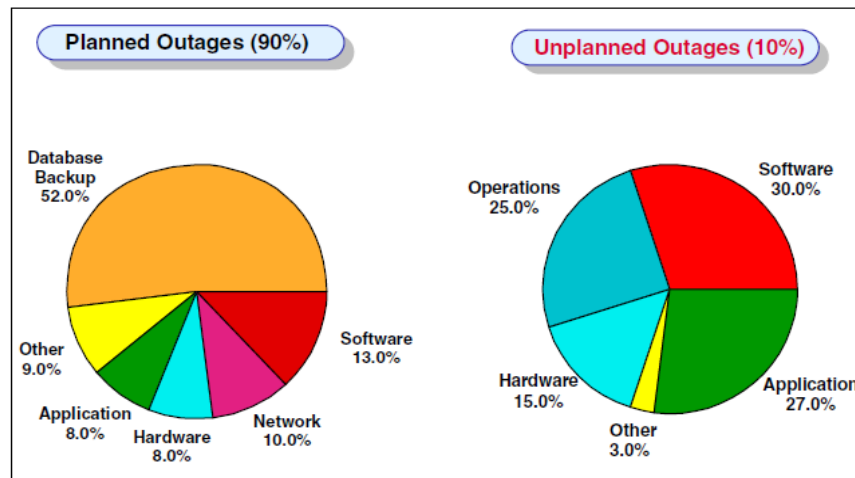


Figure 2.1: Planned versus unplanned outages for IT operations [15]

Contingency planning (CP) is defined as the totality of activities, controls, processes, plans *etc.* Relating to major incidents and disasters. It is the act of preparing for major incidents and disasters, formulating flexible plans and marshaling suitable resources that will come into play in the event, whatever actually eventuates. The basic purpose of CP is to minimize the adverse consequences or impacts of incidents and disasters. There are a number of more specific terms and activities included under the broad concept BC and disaster recovery planning is one of the main component of CP which focuses on the IT infrastructures and operations [16].

A BCP consists of the following component plans:-

- ❖ Business Resumption Plan
- ❖ Occupant Emergency Plan
- ❖ Incident Management Plan
- ❖ Continuity of Operations Plan
- ❖ Disaster Recovery Plan

The Incident Management Plan (IMP), which does deal with the IT infrastructure, establishes structure and procedures to address cyber-attacks against an organization's IT systems and generally does not involve activation of the Disaster Recovery Plan. The main focus study was about ITDRP which is one of the integral part business continuity plans which ensure the existence of organizations during and after disasters. ITDRP It's part of the business continuity program but is focused on the assets, people, processes, and technologies involved in critical aspects of business operations.

ITDRP is a logical subset of the BCP process, which focuses on continuity of IT operations. But ITDRP also includes key non technology assets, people, and processes in recovering from a disruptive event [17].

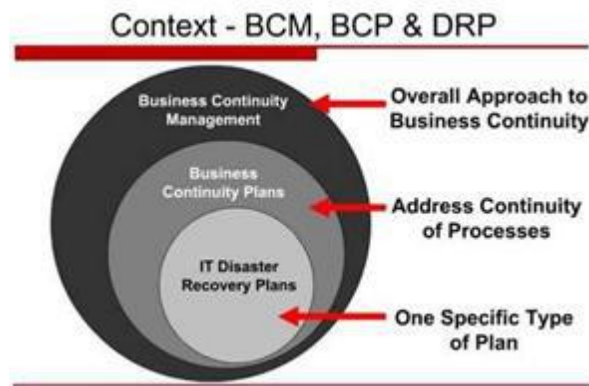


Figure 2.2: BCM, BCP & DRP Context [13]

ITDRP contains of defining rules, processes and disciplines to ensure that mission critical businesses will remain available to function even if a disaster is occurred [7].

The following are the key elements to ITDRP:-

- ❖ Establish a planning group
- ❖ Perform risk assessment and audits
- ❖ Establish priorities for applications and networks
- ❖ Develop recovery strategies
- ❖ Prepare inventory and documentation of the plan
- ❖ Develop verification criteria and procedures
- ❖ Implement the plan

Comprehensive disaster recovery planning should include different elements beyond the IT department walls, so the group members of the project team should include expertise from different departments. The following diagram shows the main elements that disaster recovery planning should address.

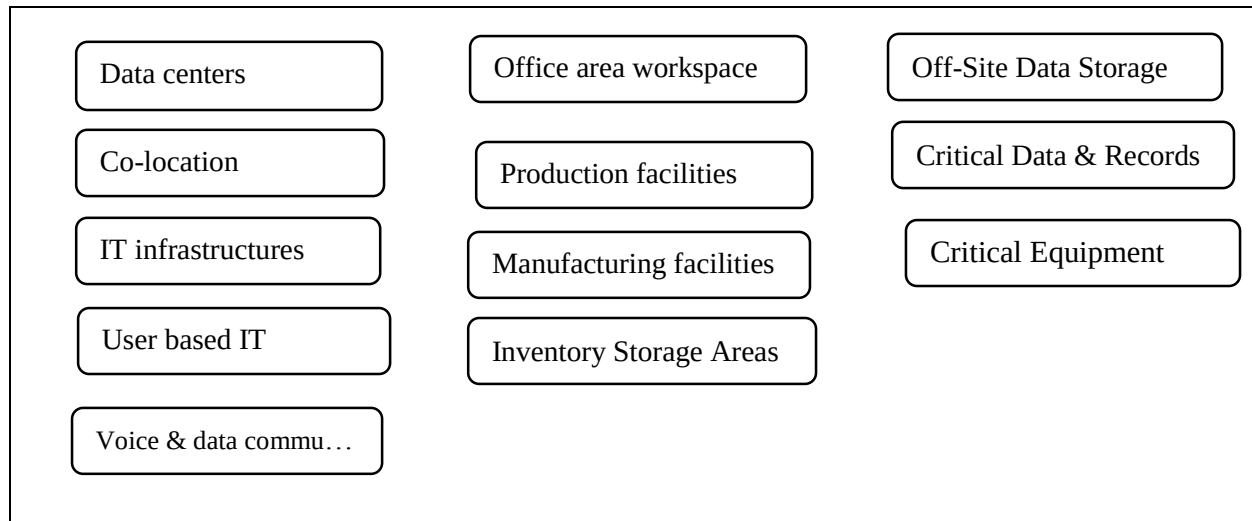


Figure 2.3: Elements of disaster recovery plans [12]

2.2.1. IT Disaster Recovery Plan Components

For the purpose of ITDRP there are three main elements, people, process, and technology. During DR planning these three elements are very important to implement the DR system. Technology is implemented by people using specific process. Whereas process is a defined way to accomplish the task. But technology is only as good as people who designed and implemented it and the processes developed to utilize it.

- ❖ **People**, are the ones who do the actual planning and implementation disaster plan. But the people participated in the DR planning should not restricted to IT department but it should also include from the other departments and managerial position.
- ❖ **Process**, is a properly documented steps that used to manage the disaster recovery planning tasks.
- ❖ **Technology**, are materials that used during emergency plan and it get business back up (running) and needed to manage the crisis.
- ❖ **Infrastructure**, sometimes it can included in the technology segment of people, process and technology but mostly used as discrete catagory in IT DRP.

2.1.2. IT Disaster Recovery Planning Processes

Preliminary Literatures has discussed about the different planning steps used in developing disaster recovery strategy. And IT Disaster Recovery planning process is one of disaster recovery plan that apply the seven steps [12]. They are as follows:-

1. Develop the Business Contingency Planning Policy and Business Process Priorities
2. Conduct a Risk Assessment
3. Conduct the Business Impact Analysis
4. Develop Business Continuity and Recovery Strategies
5. Develop Disaster recovery plan
6. Conduct awareness, testing, and training of the DRP
7. Conduct Disaster Recovery Plan maintenance and exercise



Figure 2.4: Disaster recovery planning phases [12]

Stage	DR title	Process
1	Project initiation	It clearly set the main objectives and establishes the basic component of the project. An effective project initiation process helps assure the success of the IT DR plan [12] [15].Some of major tasks include in this stage are as follow: • Project organization • Forming the project team • Clearly define project requirements etc.

2	Risk assessment	Risk assessment evaluates an organization's IT systems regarding the possible threats and vulnerability of the systems. The main tasks under this stage are: • Threat assessment • Vulnerability assessment • Impact assessment • Risk mitigation strategy development
3	Business impact analysis	The fundamental task in BIA is understanding the mission critical tasks which keep the ongoing operations and understanding the impact of the disruption of these process on the whole business. And BIA focuses on the key departments which possess critical user data.
4	Recover/mitigation strategy	Risk mitigation is step takes to reduce adverse effect. There are four types of risk mitigation strategies which taken as to reduce possible risks. These are: • Risk avoidance • Risk limitation • Risk transference • Risk acceptance
5	Develop ITDR	Based on the information reveal in BIA process, this stage require an identification and documentation of specific policies and procedures to be used in the event of a disaster.
6	Test ITDR	Once the plan has been developed, it must be tested and audited to ensure weather it can accomplish recovery objective or not. Major tasks include: • Developing testing strategy • Training staff • Conducting testing procedures

7	Maintenance ITDR	Since change are inevitable, IT DR requires a continuous support and maintenance in order to fit the current requirements. The following tasks are required to maintain the IT DRP: • Identify the main source changes • Select change management policy • Documentation the maintaining plan

Table 2.1: The seven IT DRP phases

2.3. IT Disaster Identification

2.3.1. What is a disaster?

Over the past decade, the world has experienced a diverse range of disasters like tornados, tsunamis, droughts, cloud bursts, floods, cyclones, typhoons etc. highlighting the huge demand for Business Continuity [13]. To better assist in disaster preparedness and economic recovery it is important to have an understanding of disasters. A disaster is any event that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operations of the business. Disasters can take many different forms, and the duration can range from an hourly disruption to days or weeks of ongoing destruction.

The cause of disasters can be classified in to three main categories:

- I. Natural hazards
- II. Human-caused hazards
- III. Accidents and technological hazards

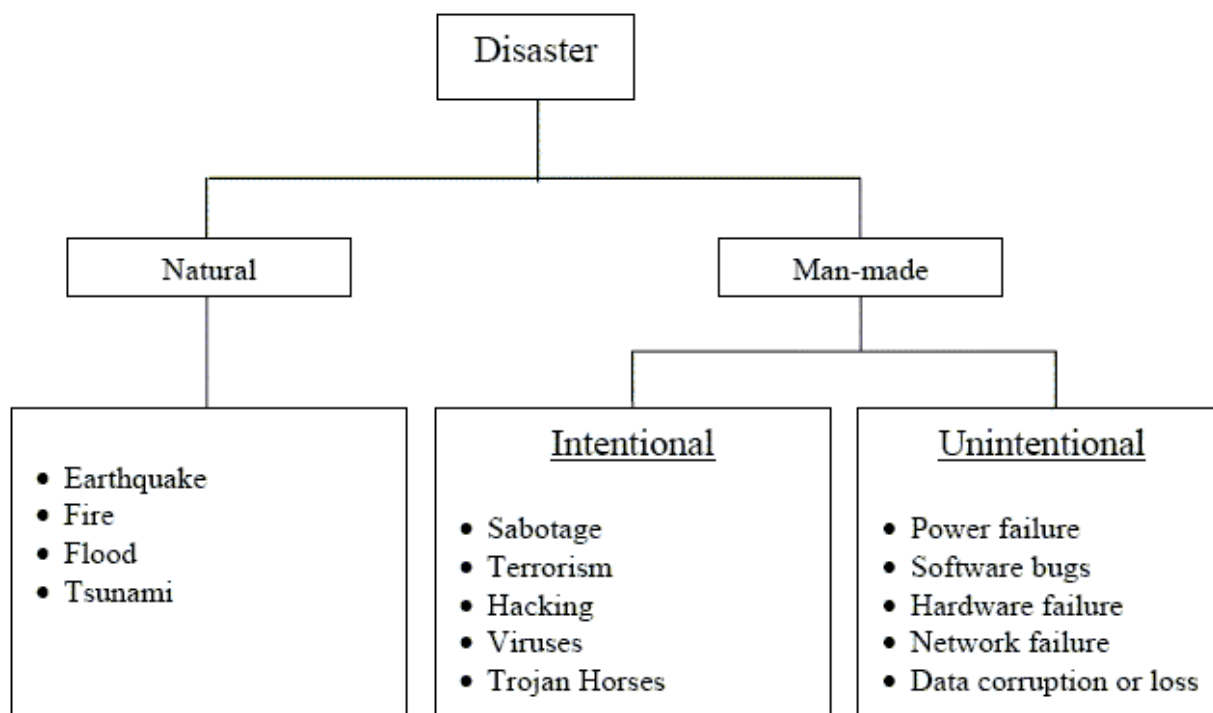


Figure 2.5: Model of Types of Disasters [18]

I. Natural Disasters

Natural disasters are type disaster that would come through the natural phenomenal and its consequence could be seen in the business organization including the banking. But they can avoid the effects of the natural disaster by having DRP in place. Natural disasters range from fire to hurricane that could destroy the whole organizations in a given place. The following are the type disaster that included in natural disaster:

- Rain and wind storms
- Floods
- Biological agents
- Earthquakes
- Volcanic eruptions

II. Man-Made disasters

Man-Made disasters are types of disaster that caused by human beings. The disaster caused by human beings could be intentionally and unintentional. The following are some of disasters caused by human being:

• Hazardous materials • Power service disruption • Nuclear power plant and nuclear blast • Radiological emergencies	• Chemical threat and • Terrorism • Bomb • Explosion • Civil unrest
---	---

Table 2.2: Examples of man-made disasters

III. Technological Disasters

Technological hazards often are related to man-made hazards but differ only in that they are usually unintentional [12]. If intentional, they fall under the category of man-made hazards. The following category could technological disaster if they occurred unintentionally.

- Power outage
- Gas leak
- Software and hardware failures
- Electrical shortage

Disaster overview assists in understanding the phases of a disaster to help officials recognize the different stages of a disaster and better plan for, and recovery from an event. It is also important when planning or recovering from an event to understand the types of disaster.

2.4. IT Disaster Recovery Plan in Financial Industry

ITDRP is a documented process or set of procedures to recover and protect a business IT infrastructures in the event of a disaster. As business organizations are highly depend on IT, it is no longer an option to have ITDRP in place [8]. It is not possible to predict what may strike when. In today's world, it has become mandatory to prepare for such disaster scenarios always. Nowadays financial institutions are highly dependent on computerized system than ever on their key business

processes. BC in IT is the uninterrupted availability of IT resources that support key business functions. Financial losses from natural disasters continue to rise, with developing countries and their low income populations feeling the greatest effects. Direct financial loss reached an average of \$165 billion per year during the last 10 years, with loss exceeding \$100 billion in six of those years. This compares to about \$130 billion of official development assistance in 2012 [19].

Reliable IT services have become an integral part of most business processes including the banking sector. These days, it's difficult to find corners of financial institutions that technology does not touch. As a result, they need to have DRPs to recover the mission critical functionalities of the organization during and after disaster. The importance of DRP for financial sectors is undeniable especially after the 911 terrorism attack and many natural disaster experienced by different countries; then much effort has been exerted towards the set of workable DRP [20]. However, high investment is allocated for IT and DRP, there are still IT service outages interrupted the business, crippled the operations and impacted the overall organization long term strategic plan. Organizations maintaining business dynamism and attain competitive edge in the global scene are getting challenging due to the demanding stakeholders and keen competition. Sustaining uninterrupted business operation is a key in an organization's strategic plan to maintain competitive edge.

2.5. The Importance of IT disaster recovery plan for Banks

Nowadays IT disaster recovery plan is very essential for the banking sector if it is well planned, documented, and continuous revised and audited. An effective disaster recovery plan should ensure that an organizations can quickly recover their data after the emergency [8]. As banking are one the leading service industry rely heavily on IT for day-to-day activities and for the management purpose. Therefore, the importance of IT continuity, incase unforeseen situations, it has become a point of critical importance [13]. ITDRP also increased the competitive advantage of the banks if they have it in place. Because ITDRP can helps an organization to give flexible and effective service for customers during and after the emergency/disaster time. Preparing such plan also forces company to accounting applications into critical and non-critical categories. Generally, IT DR planning enables a company to quick restore its capability to process mission critical information [21]. An effective IT DR can address the following situations:-

- Loss of IT infrastructures or connectivity for an extended period of time
- Loss of critical information accounts

- Loss of access or use of the data center for an extended period
- Loss power supply for long time

2.6. IT Disaster Recovery Strategies

Different literatures had highlighted on the main disaster recovery phases. According to the 4th NASA's international workshop there are four main phases during DRP [21]. They are as follows:-

- Prevention
- Preparedness
- Response
- Recovery

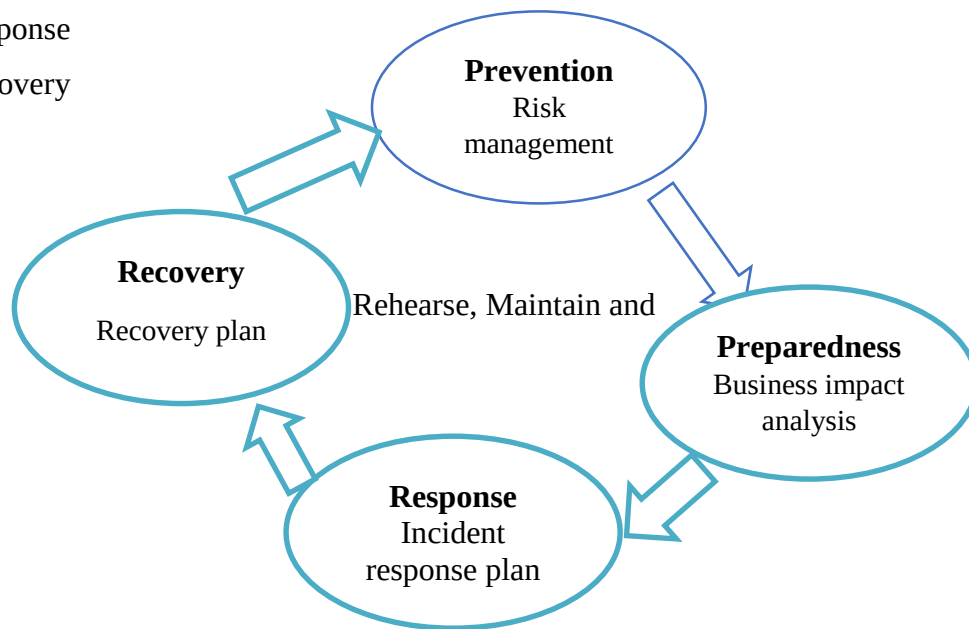


Figure 2.6: IT Disaster recovery plan phase [22]

1. Prevention

This action is taken to reduce or eliminate the like hood effects of the disasters. This phase always come first before the others phases to avoid potential loose of critical business functions and always covered by the risk management planning group.in this phase it mainly covered ,the risk identification, the possible threats, and the impact of threats on the IS system and mission critical services of the organization.

2. Preparedness

This is second phase which focused on taking action prior to actual incident occurring to ensure an effective response and recovery. It also shows the general readiness of the organizations in different aspects including designing the DR planning with the required facilities and skillful

professionals that manage the DR system. Preparedness is all about being proactive and planning and BIA largely captures the preparedness aspect. Business Impact Analysis is one core tasks during preparedness which deals with the basic recovery requirements for the organization during the crisis. BIA used to establish critical business activities, required resource to support each activities, impact the incidents to perform the activities and the Recover Time Objective assigned to each mission critical activities.

3. Response

This phase used to respond the incidents immediately after it happens. The response phase covers the actions containment, reducing damages of the infrastructure and preventing the incident escalation. Generally response phase involves an operational management and communications response and incident management response is largely responsible for this phase.

4. Recovery

This is the last phase (action) which is responsible to recover or restore the system after incident happened but this may not always possible to recover. Recovery can broadly classified in two, resumption (continuity) of business activities Restoration (recovery) of resources.

2.7. Tiers of IT Disaster Recovery Plan

According to International Business Machines (IBM) report there are seven tiers of disaster recovery strategies used to fit different organizational recovery solutions [15]. But understanding and selecting the DR strategies and solutions is can be complex for companies. The seven tiers DR categorized based on different characteristics such as, costs, recovery time capabilities, recovery point capabilities.

These three questions are very important before we go for selecting the ITDRP strategies.

- What kind of solution they have?
- What kind of solution they require?
- What it would require to meet greater ITDR objectives?

The seven tiers ITDR are as follow:-

1. Tier 6 - Zero data loss
2. Tier 5 - Two-site two-phase commit
3. Tier 4 - Electronic vaulting to hot site (active secondary site)
4. Tier 3 - Electronic Vaulting
5. Tier 2 - Offsite vaulting with a hot site (PTAM + hot site)

6. Tier 1 - Offsite vaulting (PTAM)
7. Tier 0 - Do Nothing, No off-site data

The following section provides an overview of each tiers and describing their characteristics and associated cost. And Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are the two very important concept related recovery capability strategy are also noted in each tier.

Tier 0 - Do Nothing, No off-site data

On this tier nothing is done, and it defined as a single site data center environment having no requirements to backup data or implement a Disaster Recovery Plan. On this tier, there is no saved information, no documentation, no backup hardware, and no contingency plan. Generally there is DR capability at all.

Tier 1 - Offsite vaulting (PTAM)

A Tier 1 installation is defined as having a ITDRP, backs up and stores its data at an offsite storage facility and has determined some recovery requirements. Data are back up to offsite storage facilities. But this tier does not have alternative site and required hardware on which to restore the data. This tier is described as Pickup Truck Access Method (PTAM). PTAM is a method used by many sites, as this is a relatively less inexpensive. However, it is difficult to manage and complex to know exactly where the data is at any point.

Tier 2 - Offsite vaulting with a hot site (PTAM + hot site)

Tier 2 embraces all requirements of Tier 1(offsite vaulting and recovery planning) plus it include the hot site. On tier 2 the hot site has contains all sufficient hardware and network infrastructure that able to support the installations of critical processing requirement. Tier 2 installations rely on a courier (PTAM) to get data to an offsite storage facility.in the event of disaster the data at the offsite storage facility is moved to the hot site and restored onto the backup hardware provided. But moving data to the hot site is increase costs and decrease the recovery time significantly.

Tier 3 - Electronic vaulting

Tier 3 encompasses all the requirements of tier 2 (offsite backups, disaster recovery plan, hot site) and in addition supports electronic vaulting of some subset of the critical data. Electronic vaulting

consists of electronically transmitting and creating backups at a secure facility, moving business-critical data offsite faster and more frequently than traditional data backup processes allow. The receiving hardware must be physically separated from the primary site and backups are being taken and they are then being stored at an offsite storage facility.

Tier 4 - Electronic vaulting to hot site (active secondary site)

Tier 4 is defined as using two data centers with electronic vaulting between both sites and introduces the requirements of active management of the data being stored at the recovery site.

This is managed by a processor at the recovery site and can support bi-directional recovery. The receiving hardware must be physically separated from the primary platform. There is also continuous transmission of data or connection between the primary site and the hot site, supported by high bandwidth connections.

Tier 5 - Two-site, two-phase commit

Tier 5 encompasses all the requirements of Tier 4 (offsite backups, disaster recovery plan, electronic vaulting, and active secondary site), and in addition, will maintain selected data in image status (updates will be applied to both the local and the remote copies of the database within a single-commit scope). Tier 5 requires that both the primary and secondary platforms' data be updated before the update request is considered successful. Tier 5 also requires partially or fully dedicated hardware on the secondary platform with the ability to automatically transfer the workload over to the secondary platform.

Tier 6 - Zero data loss

Tier 6 is the ultimate level of disaster recovery which is known as zero data loss. Tier 6 encompasses zero loss of data and immediate and automatic transfer to the secondary platform.

Local and remote copies of all data are updated and dual online storage is utilized with a full network switching capability. The two systems are advanced coupled, allowing an automated Switchover from one site to the other when required. This is the most expensive Disaster Recovery solution as it requires coupling or clustering applications, additional hardware to support data replication, and high bandwidth connections over extended distances. However, it also offers the speediest recovery by far. Figure 2.7 below shows length time require by the seven tiers.

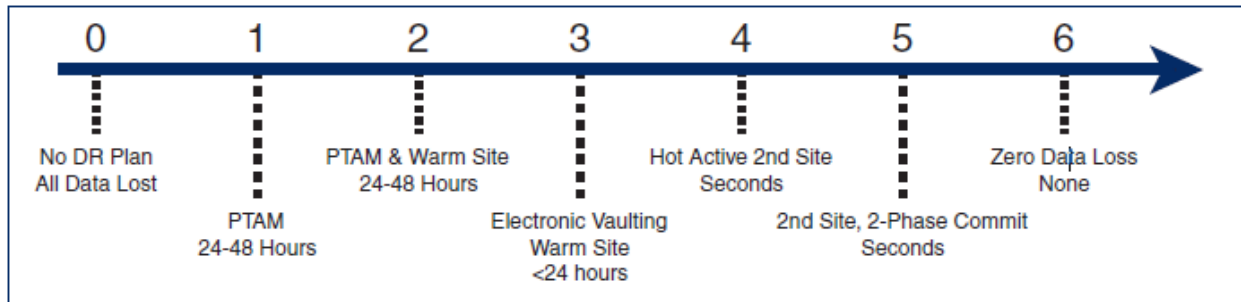


Figure 2.7: The typical length of time for the recovery in seven tiers [8]

2.8. Types of IT Disaster Recovery Techniques

Alternative site is a premises where computer hardware and network infrastructures used to processes data and provide service to user when the primarily location failed to perform its usual function because of disaster strike. According to [4] [15] there are several alternative disaster recovery sites that implement at different level of recovery capability. The disaster recovery site can be varied from one organization to another organization depending on the business requirements and affordability. The above 7 tiers of ITDR have been defined and categorized in to four main alternative disaster recovery sites. The main different among these four options is mainly goes to the recovery time and cost of their ITDR site. The four categories of ITDR sites are discussed as follow:

- **Cold site:** This is an alternative location consist of a facility with adequate space and fully infrastructure including electric power, telecommunications and environmental controls. But the site does not contain IT infrastructures needed for operations. Cold site is usually designed for an organizations that have high tolerance downtime. The recovery time of this site is very much with compare to other DR sites, but it's the most inexpensive to build.
- **Warm site:** This sites provide fully facility location and IT infrastructure and equipment to restore the business critical operations. Mainly this site contains all power and environmental services are in place, along with hardware, software, and network components needed for operations. Warm site is appropriate for an organization which have moderate level of tolerance downtime. However, there are limited staffs operate at this site because high overhead cost [4]. In warm site the RTO should be with one day whereas RPO could up to 5-30 minutes.

- **Hot site:** Contains a location which is fully equipped with IT infrastructure such as servers, storage, network and software systems [15]. For this site full time manpower or vendor support is required for 24/7 operations. Therefore, IT and processes oriented resource should be available and ready at the location on a standby mode. The acceptable maximum RTO and RPO would be within 12 hours and 10 minutes respectively [4].
- **Mirrored site:** This site is more similar to the primary location which is fully furnished with IT infrastructure and communication links. Mirrored site provides highest level of availability because data written and stored synchronously at both sides [15]. Mirrored site build and maintained at approximately double price of the production data center facilities. Due to its high availability remote users may not recognize from which data center they are actually accessing. Any data loss is not accepted at mirrored sites and RTO can be up to 1 hour. Table 2.3 summarizes the criteria that can be used to determine which type alternative site meets the organization's business need and BIA requirements.

Site type	Capital costs	Hardware / software	Network / communication	Setup time
Cold	Low	None	None	Days/weeks
Warm	Medium	Partial	Partial/full	Days
Hot	High/Medium	Full	Full	Hours
Mirrored	High	Full	Full	Minimum

Table 2.3: Alternate site decision criteria [15]

2.9. Selecting ITDRP Testing Methodologies

In order to evaluate the effectiveness of the ITDRP plans and to check whether the plans are working according to the business needs or not, ITDRPs should be tested and reviewed continuously. Each business-critical defined in the plan should be completely reassessed based on the BIA and Residual Risk (R_R) determined via Risk Analysis (RA) of threats, vulnerabilities and safeguards [23]. The development of an effective testing process is important to ensure that staff are familiar with the recovery measures deployed and that the procedures are updated and relevant. The ITDRP should be tested on an annual basis or after a major update to the technical environment [24].

ITDRP testing can consist different types of approaches, but the following are some the widely used approaches:

- **Table top-** this testing involves the owner/top manager and subset of the users of the plan to read over the plan in detail, and ensure that the information contained remains factually correct and should theoretically continue to provide effective recovery.
- **Walk through-** is a type of testing that a team member verbally “walk through” the specific procedures as documented in the plan to ensure effectiveness, identify gaps and major bottle necks of the plan. This test works in conjunction with previously validated checklist plans. This test provides the opportunity to review with large subset of people and allowing staffs to be familiarized with the procedures, equipments and offsite facilities if required.
- **Isolated simulation-** this test involves live activation of the teams and plans using a realistic and hypothetical scenario limited to the specific application and associated infrastructure.
- **Integrated simulation-** this exercise involves live activation of the teams and plans using realistic and hypothetical scenario including multiple application and associated infrastructures to test the ability of to recover each critical application with its business requirements when service outage occurred.
- **Full simulation-** this exercise involves the live activation of the team across more than one level of the organization using realistic and hypothetical scenario all mission critical application. This is the most robust examinations and realistic for the team and plans.
- **Parallel testing-** is a type of testing that can be performed in conjunction with checklist tests or simulation tests. Under this testing, historical transactions such as prior business day’s transactions are processed against the preceding day’s back up files at the contingency processing site or hot site. All the results produced at the alternative site for the current business date should agree with those results produced at the alternative site.

- **Full interruption testing**-this test activates the whole ITDRP,however,this test could disrupt the normal operation and it should be approached with caution.

During testing cycles checklists plays a major role in validating the ITDRP based on the business requirements.Checklists are less expensive tools that used to implement and maintain and provide the backbone of the testing cycle. Figure 2.8 depicts the good fit ITDRP teting cycle scenario.



Figure 2.8: Illustration of an ITDRP Cycle Testing Scenario [23]

2.10. Standards and guidelines for IT disaster recovery plan

This topic presents different international standards and guidelines use for designing a comprehensive ITDRP. The following are some of the international standards commonly used to design all-inclusive ITDRP for financial institutions. The international standards and frame work include such as COBIT, ITIL, ISO/IEC 27k, and NIST.

A. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) is an international organization which create standards and policies regarding the IT DR and business contingency of an organization. For example ISO/IEC 22301:2012 was the word's first international standard established for BCM to assist organizations minimizes the risk of business disruption , ISO/IEC 27031 contain guidelines for ICT readiness and business continuity and ISO/IEC24762 is for IT disaster recovery services [25].

B. Control Objectives for Information and Related Technology (COBIT)

COBIT is a framework developed by Information Systems Audit and Control Association (ISACA) for IT management and IT governance. It mainly supports manager to bridge the gap between control requirements, technical issues and business risks [13] [25]. COBIT 5 is a framework that provides comprehensive guidelines that assist enterprises to achieve the goals and deliver values through effective governance and management of enterprise IT. However, this framework is mainly established for BCM Audit/Assurance Program, IT Continuity Planning Audit/Assurance Program. COBIT enables business executives to better understand how to direct and manage the enterprise's use of IT and the standards of good practices to be expected from the IT providers.

COBIT 5 addresses all the management of information and related technology from an enterprise-wide and end-to-end perspective as indicated in the figure 2.9 below.

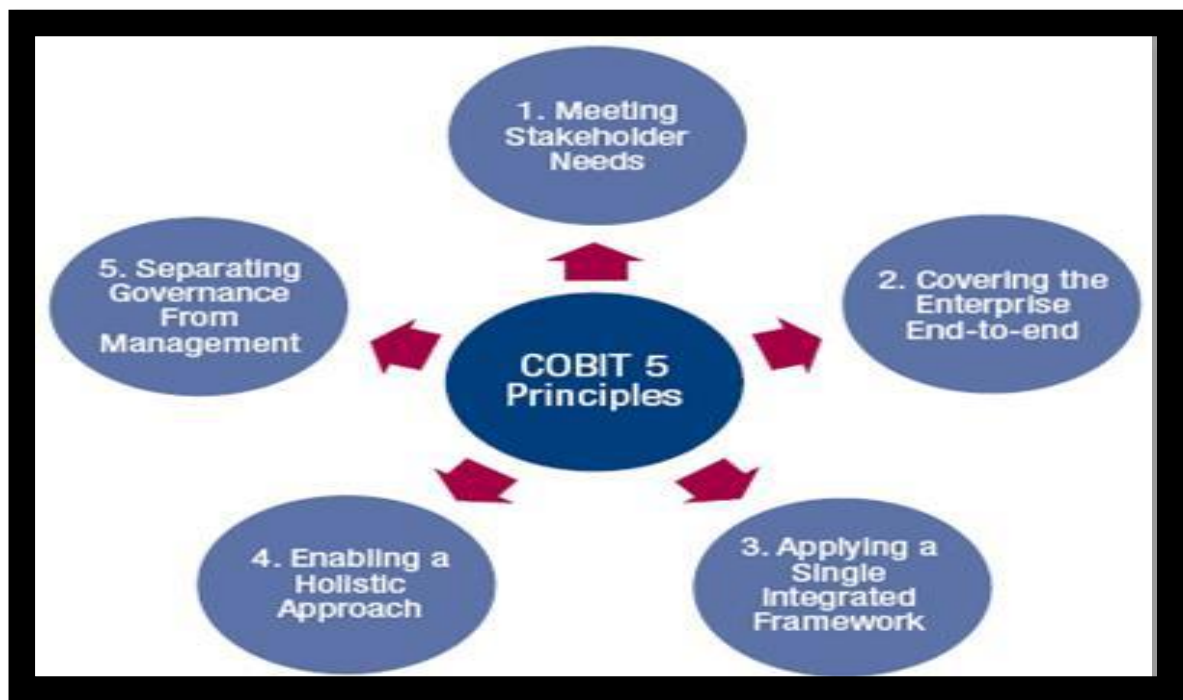


Figure 2.9: COBIT Principles [13]

C. Information Technology Infrastructure Library (ITIL)

ITIL is a standard published by the UK government which established a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business [26]. This

framework also contains guidelines for BCP process and documentation. There are five stages in ITIL service lifecycle:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

The figure 2.10 depicts the frame work of ITIL along the five stages of ITIL service life cycle.

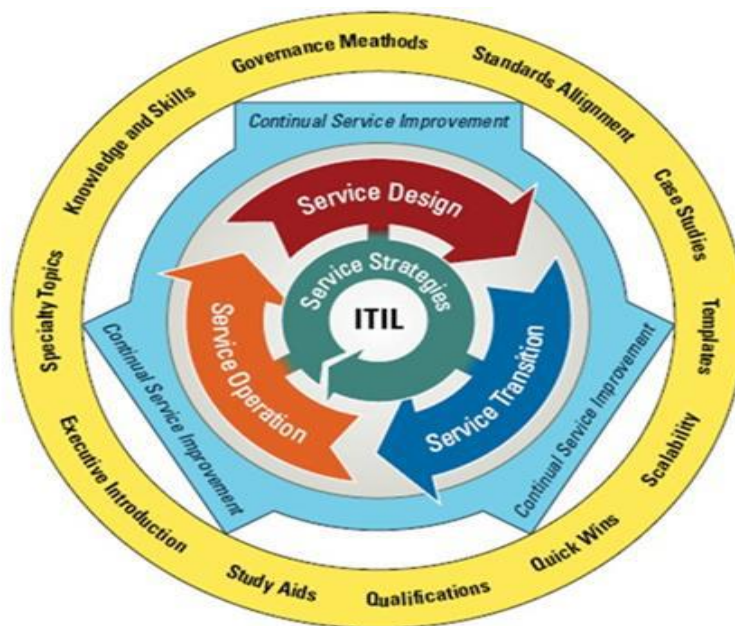


Figure 2.10: ITIL frame work [13]

The following are some of the benefits of ITIL for customers/users:

- The IT services are described better in more detail
- The quality, availability, reliability and cost of the services are managed better
- The provision of IT services becomes more customer-focused

Some of ITIL benefits for IT organization are:

- The IT organization develops a clearer structure, more focused to the corporate objectives
- The IT organization has better control of the IT infrastructure and services
- ITIL provides the quality internal communication and communication with suppliers.

D. National Institute of Standards and Technology(NIST)

NIST is responsible for developing standards and guidelines for providing adequate information security and for all operations and assets. It's created by the federal government of US and it has series of Special Publication (SP) Federal Information Processing Standards (FIPS) that provide federal agencies with standards and guidelines for most aspects of information systems security. NIST SP 800-34 – was the first publications for IT contingency planning guideline and provides instructions, recommendations, and considerations for government IT contingency planning.

There are also other best practices and guidelines used for national wise such as ICT Readiness for Business Continuity (IRBC), British standard (BS25999), IT Governance Framework, and RBI for Indian bank.

2.11. Related works

This section covered the different research works that has been done so far on related to objective of the study.

The preliminary literature in [27] was prepared in Zambia commercial bank and this paper is entitled with “investigation into the effectiveness of Business Continuity Plans for Commercial Banks in Zambia”. The author has begun his discussion with the historical back ground of banking sector, the start of financial reform, the current form the banks and importance of banking sector for the Zambian economy. As the main objective of the study is to investigate the effectiveness of business continuity plan for the commercial bank in Zambia. The author has discussed in detail about the definitions, characteristics, components and recovery strategy of BCP. As the author cited from Business Continuity Institute, BCP defined as a documented collection of procedures and information that is developed compiled and maintained in readiness for use in an incident enable an organization to continue to deliver its critical products and services. It was assumed all the individual commercial banks in Zambia has BCP in place but by that time it is not known whether the plans are effective or not for the intended purpose. In order to find the missing link the author has devised the primary and specific objectives clearly. Therefore, the study was proposed to investigate the effectiveness of BCPs for the commercial banks in Zambia and to ascertain whether the plans are incorporate with corporate strategies and they conform to international standards. The study was designed to answer the main research questions such as, does each commercial bank have a BCP, how the plans are incorporated in corporate strategy; how

often does plan tested, review, updated and audited and to which standard are plans benchmarked. The author has used both quantitative qualitative research methodology address the objectives of the study. The study was targeted at fourteen (14) commercial banks in Zambia. For the qualitative method, the author has used observation, document analysis and semi-structured interview as data collection instrument. Whereas for the quantitative method he used such as, questionnaire, guided oral interview and desk research. The questionnaire were distributed to head Department of Information Technology, Security and Risk Management. The quantitative data were analyzed by SPSS whereas the qualitative were organized and analyzed manually. Following the investigation the author found that except one local all banks have BCP in place. However, some of the banks were indicated that their plans are not well understood by the employees. Almost all the banks in Zambia tested their plans' in every three months, six months and annually. Generally the author has stated that most of the banks in Zambia has BCPs in place but it didn't actually well understood by the employees. And the respond from participants in both questionnaire and interview indicated that they have frequent mechanisms to test and audit their plans. However, almost all the banks in Zambia have not well understanding about the different DRP standards.

The research in [28]discussed about the fundamental aspect BCP, ITDRP and anticipated disasters with their possible impacts and the importance of ensuring the BC. The author admitted that there was huge progress in IT in the past decade, but he can't hide that possible IS threats are not well considered so far as necessary. And the author indicated that there is still lack of preparedness of business continuity in some companies because of lack awareness about the plans and underestimating the possibility occurring of disasters. As the objective of the paper is to give insight about the relation and importance BCP&DRP to Information Systems; the author described clearly about the definition, components, process, significance and the recovery strategies of the plans. In this paper the author also discussed about the nature of the disaster cause including, natural, human made and technical causes and the possible disaster impacts on the entire organization. Finally, the author established the possible way to design ITDRPs and the challenges that affect the effectiveness of the plans.

The article in [29] investigated the business continuity and disaster recovery plan in electronic based banking based on different litratures that have been done before in the banking sector of

Indian. As it indicated in the literature, the main objective of study is to observe whether the banks in India have effective disaster recovery plan in place or not as per Reserve Bank of India (RBI). The authors highlighted that banks in India have disaster recovery plan but it is not known whether the plans overwhelm the possible disaster occurrences. The authors have used both types of data sources that are the primary and secondary in order to achieve the objective of the study. The comparative study undertaken in nine different commercial banks of India that have been selected based on random sampling technique. The qualitative data was analyzed using the statistical analysis tool called GAP. Finally the researchers found that all the selected banks have BCP and IT DRP in place that meet the specifications set by RBI. And they suggested that, these requirements may be considered as core-technical elements of IT disaster recovery plan and includes activities such as creating backup, acquiring technologies, and developing ways of resuming services. But the authors also describes the vital components beyond these core-technical elements should be taken into consideration like creating IT disaster response teams, training personnel, warning employees of disasters, establishing communication channels, and formalizing decision-making authority.

According to the authors [9] the advance of the banking sectors brings in an era of multi-products and multi-services being delivered using multiple yet integrated channels. And they stated that the use of ICT is on increases and encompasses almost all the banking operations. The objective of study is to identify the essential ingredients of successful Business Continuity Management (BCM) the experience in Indian banks. As the authors defined, BCM is a methodology that could be used by organizations to reduce the risks that occur at organization level and its outside environment.

As they cited from previous literature, most organizations, including banks, in Maharashtra nowadays depend on the information technology on their key business functions. In fact, IT considered as vital component for conducting business activities. But the failure of IT component in organization could directly affect the business activities. Consequently, upon this understanding, organization top management should take the right actions the continuity of information technology services. The disaster recovery plan should interface with overall business continuity management plan, be clear and concise and focus on the key activities required to recover the critical IT services. The major purpose of the study was to identify the internal and external qualitative factors that affect managerial decision on BCP life cycle process. Thus, the study is

designed to answer the three main research questions, including what internal and external factors that affects the decision making process during the BCP lifecycle to be identified and how the these factors be employed to present an assessment model for decision making process in banking organizations in Maharashtra. They have been used the qualitative data that extracted from the survey which then formulated into another quantitative data. Finally, the result of the analysis were organized and series of benchmark were established. But the benchmark were related to IT disaster recovery plan activities and not part of the actual plans.

The research in [4] was aimed to develop disaster recovery framework for Sri Lanka commercial banks and asses the IT DR practices. According the researchers these six things are the most common cause for system down time such as, Software defects/failures, Planned administrative downtime, operator errors, hardware outages/maintenance, building/site disasters (i.e. Fire), metropolitan disasters (i.e. storms, floods). And the researchers discussed about the different DR methods, processes and essential factors to design proactive IT DR that help an organizations to survive and continues their business during and after emergency. Furthermore, the researchers analysis the different international standards that help to develop the new IT DR framework for commercial bank of Sri Lanka, the standard include such as ISO/IEC24762:2008, BS 25999 and ISO 27001. The result of the research indicated that the most of the banks in Sri Lanka have adopted IT DR strategies that supported by the regulatory guidelines of the central bank but the viability of the plan questioned. Generally, the researcher understands the current IT DR in Sri Lanka commercial banks are not feasible and not well supported by international standards. Due to that they proposed new IT DR framework which helps top level manager to devise step-by-step procedure to develop and set up IT DR practices for their respective banks. Previous literatures reveals that research on IT DRP focused on the presence of the plan in financial institutions (banks), developing comprehensive IT DRP frame work, and examining effectiveness of the plan but according the literatures this area of research still has receives little attention. However, in Ethiopia there is no any related local works done so far related to IT DR experience in financial institutions including banks. Tables 2.4 below shows the summary the related works on IT DRP exercise in banking sector with their research methodology and major findings.

Authors	Objectives	Methodology	Major findings
Musonda Simwayi (2008)	To examine the effectiveness of BCP for commercial banks of Zambia and over view of BCP in relating to the banking sector	Qualitative and quantitative was used	Except one local bank all the banks in Zambia have BCP in place but more than halve of the BCP are no effective. And most of the banks didn't have clear understanding about the different BCM standards.
Tejinder Pal Singh Brar, Dhiraj Sharma, Sawtantar Singh Khurmi (2016)	To observe weather the selected bank in India have effective IT DR and BCP in place	Qualitative and Quantitative approach are applied using structured interview and survey questionnaire	All the banks regularly bank up their data on offsite location but they don't applied IT-DR as per RBI guidelines and international standards. And most of the banks found they don't have disaster avoidance committee
ShirshenduMaitra, Dr. Meera Shanker, PankajK. Mudholkar(2013)	Identifying internal and external factors that affect decision making process during BCP life cycle in bank organizations	Qualitative approach which then formulated in to quantitative data	Most of the bank consider state-of-the-art technology as critical to growth and efficient delivery of service. Customers and partners provides strong support during the phase when the bank attempting to recover from a disaster.
Mueen Uddin, Sandun Hapugoda, Roop Chand Hindu(2015)	To assess the DR practices and develop frame work for commercial bank of Sri Lanka	Qualitative approach using structured interview	Though the banks have IT DR in place but they are not supported by international standards and guidelines

Table 2.4: summary of related works

2.12. Chapter summary

This chapter presents the relevant literatures related to the objective of the study. It mainly focused on reviewing the literatures related to ITDRP components during prevention and recovery processes. Specifically, this chapter presents the key components of ITDRP, potential threats, ITDRP processes, recovery strategies, alternative site, testing types, guideline and standards used to design ITDRP. And different related works were reviewed and summarized under this section.

Chapter Three

3. Research Methodology

3.1. Introduction

The research method is systematic way in which that defining the objective, managing the data, and communicating the findings occur within established frameworks and in accordance with existing guidelines [30]. The purpose of this chapter is to design appropriate research methodologies that are used to carry out the study in line with of the research objectives and research questions. This chapter discussed about the research approaches, target populations, data collection instruments, instrument validation, reliability and data analysis approach that are applied for analyzing the collected data. The chapter also discussed the procedures used during survey, and ethical issues to be considered during distribution and analysis of the collected data.

3.1. Research design

Research design is a master plan used to specify the methods and procedures for collecting and analyzing the required data [31]. The research approach for any study is always selected based on the research problems, objectives and research questions. Since the objective of the study was to examine the current status of ITDRP in Ethiopian banking sector. There are three common approaches used to conduct research these are qualitative, quantitative and mixed methods [32]. The quantitative research method involves numeric and statistical approach and it maintains empiricist paradigm. The quantitative research method has three main broad classification descriptive, experimental and causal comparative. Qualitative approaches stress the importance multiple of subjective realities as importance source of the data [33]. Therefore, the study used both, quantitative and qualitative methods which often called mixed research design to collect the relevant data and to draw meaningful conclusion about this study.

In this research the qualitative part was mainly used to clarify data responses from open ended questions in the questionnaire. In this way, it was also used to meanings over the statistical value of quantitative findings. In this study the descriptive statistics was used in order to carefully examine the situation, as it exists in its current state. Descriptive research is explained as statement of affaires as they are at present with researcher having no control over the variable. Therefore,

simple descriptive statistics, namely percentage, table, figure and charts were used to explain situations pertinent to current status of ITDRP in Ethiopian banking sector.

3.2. Target population

The target population for this study was individuals (IT directors) who were the staff members in all the banks' head office located at Addis Ababa city. As the number of banks in the city were small, census sampling was used to include all the nineteen IT directors in each of bank head offices located at Addis Ababa.

However, the reason for selecting IT directors was purposive sampling because of the profession and responsibility of the respondents they have in the head office. Therefore, purposive sampling was used to select only IT directors, though there were other staffs. Purposive sampling is non-probability sampling method, and useful of selecting samples based judgmentally on their merits or special experiences that might have in relation to the research topic [33]. Purposive sampling is also proved to be effective when limited numbers of people required to gather primary data. Therefore the researchers found that this sampling technique is suitable for selecting the nineteen candidates from the banks. The target banks were two state-owned, NBE and sixteen from private sector. Table 3.1 shows the list of all target bank's head office located in Addis Ababa:

Bank names and its category			
No.	Private Banks	No.	State-Owned Banks
1	Abay Bank S.C	1	Commercial Bank of Ethiopia
2	Addis International Bank	2	Development Bank of Ethiopia
3	Awash International Bank	3	National Bank of Ethiopia
4	Bank of Abyssina		
5	Berhan International Bank		
6	Buna International Bank		
7	Cooperative Bank of Oromia		

8	Dashen Bank	
9	Debub Global Bank	
10	Enat Bank	
11	Lion International Bank	
12	Nib International Bank	
13	Oromia International Bank	
14	United Bank	
15	Wegagen Bank	
16	Zemen Bank	

Table 3.1: list of target banks

3.3. Data Collection Methods

Data-collection techniques allow a researcher to systematically collect information and describe context of the study, where the study is conducted. Even if there are a number of data collection instruments in research, the most common and widely used are: interviews, surveys, often called questionnaires, personal observation and documentary review.

For the purpose of this study, survey method was employed to collect the necessary data about the research. Surveys can be constructed in many ways, but they always consist of two important components, questions and responses. Most of time survey type method used close ended questions, in which respondent are asked to select from a range of predetermined answer. However, they can have some open-ended questions. This is because of the fact open-ended responses are not as easy as close-ended question for coding, rather they require more resources and time to handle than close-ended items.

Although surveys are popularly referred to as paper-and-pencil instruments, this too is changing. Evaluators are increasingly exploring the utility of survey methods that take advantage of the emerging technologies. Thus, surveys may be administered via computer-assisted calling, as e-mail attachments, and as web-based online data collection systems. Even the traditional approach of mailing surveys for self-guided response has been supplemented by using facsimile for delivery

and return. Selecting the best method for collecting survey requires weighting a number of factors. These include the complexity of questions, resources available, the project schedule, and so on [32]. Survey is typically selected when answers are needed to a clearly defined set of questions. And it's good tool for obtaining information on wide range topics when in-depth probing of responses is not necessary. Survey may be administered in different ways like, Personal interview, telephone interview and self-administered questionnaire and etc. in this study, the researcher however employed a self-administered questionnaires, as all the questionnaires were distributed by the researcher himself. The questionnaire was adopted from preliminary literatures that done in similar research area in India and Zambia [9] [27]. However, little modification was made to the previous questionnaires according the purpose and research questions of the study.

3.4. Approaches of data analysis

This research used descriptive statistics data analysis approach which is suitable for quantitative values. In terms of applying specific approaches, the researcher used both quantitative and qualitative approaches of data analysis. More specifically, descriptive statistical analysis was used to analysis the quantitative data by using SPSS computer program, version, 20. On the other hand, the qualitative data were analyzed through simple thematic analysis. This was applied by organizing similar responses and themes that the respondents mentioned while addressing the open-ended questions, and then developing a category suitable for giving meanings for responses in relation to the research objectives and questions.

3.5. Research reliability and validity

Some of the main requirements of any research process are the reliability and validity of data and findings. Reliability is the consistency of our measurement, or the degree to which an instrument measure the same way each time it used under the same condition with the same area of study. According to [34] reliability mainly deals with the consistency, dependability and replicability of the result found from piece of research work. Reliability also refers to repeatability of result taken certain of populations. In quantitative research obtaining similar result could be straight forward because data are in numerical form. As the questionnaire is adapted with little modification from earlier research works it didn't involve for further testing.

Validity is always defined as the extent to which an instrument measures what it purports to measure [35]. Validity strengthens the researcher's conclusions, inferences and proportions.

Validity requires that an instrument is reliable, but can be reliable without being valid. Validity can be examined using the following common approaches these are face validity, content validity, construct validity. The researcher used content validity and construct validity to assure the validity of the instrument for the purpose of the study.

To this end, the researcher tried to give draft questionnaires for researchers and senior lecturers, who have had good experience in doing research on related topics in Wollo University. Accordingly, a number of questions were deleted, modified and re-edited as per the comments and suggestions. It was after this procedure of ensuring content and construct validity that the researcher checked the tools, and found valid and reliable.

3.6. Ethical issues consideration

Ethical considerations can be specified as one the important parts of research through the life cycle of a specific study [36].

Therefore, the following ethical issues were seriously considered throughout the entire thesis:

- The study was conducted in line with organization's policies and code of ethics regarding accessing any data resources from the organization.
- All the data were taken from the respondents with a serious adherence to principle of confidentiality and anonymity
- All the materials and resources used in this study were properly acknowledged

Chapter Four

Data Presentation, Analysis & Discussion

4. Introduction

This chapter focuses on data analysis and results discussion found from returned questionnaires. The data were collected from the IT departments of nineteen banks of Ethiopia located in Addis Ababa. Data were collected based on the research methodology framework deployed using self-administered questionnaire that contained both close ended and open ended questions about the ITDRP status, experience and deployment processes in Ethiopian banks. The researcher were distributed nineteen questionnaires to be filled by the IT directors of the respective banks and all the nineteen questionnaire were returned and filled fittingly for the purpose of the study.

4.1. Research and statistical tools employed

The research and statistical tools employed in this study are descriptive statistics and simple thematic analysis. Descriptive statistics includes frequency and percentage distributions that represents in the form of percentages, tables, charts and graphs used to present, organize and summarize the result of the analysis. SPSS, version, 20.0 was the statistical tool used to analysis the principal data attained from the nineteen banks of Ethiopia.

4.2. Analysis of the data

The data were analyzed in two parts. These are, quantitative and qualitative analysis. First, the closed ended questions were organized and nurtured in to SPSS 20.0 for analysis and to generate a meaningful results in simple frequency distribution. Second, the open ended questions were analyzed through simple thematic analysis; the responses were organized and categorized based on the similarity of responses in order to provide concrete ideas that support the quantitative results.

4.2.1. Quantitative Data Analysis from Ethiopian Banks

The purpose of the study is to examine the status, experience of ITDRP in Ethiopian banks including state-owned, private and central bank. Totally nineteen banks were involved for the purpose of the study and one self-administrated questionnaire was distributed to each of the bank's

IT department which contains five part questions that related to recovery exercise. These are as follow:

- I. Institutional data
- II. ITDRP
- III. Review of ITDRP
- IV. ITDRP Team management
- V. Financial management of ITDRP

I. Institutional data analysis

The first question under institutional data was, what is name of your bank?

See the list and name of the banks at appendix that involved in this study.

The second question under institutional data was, what position do you currently hold?

All the respondents involved in this questionnaire are worked as IT director of the banks.

Finally, the third question was, in which category do your bank fall?

According this survey currently 84.2 % (16) of banks are private and 15.8% (3) banks are state-owned banks including the central bank. Table 4.1 shows the percentages of distribution among the private and state-owned banks.

		Frequency	Percent	Cumulative Percent
Valid	Private	16	84.2	84.2
	government	3	15.8	100.0
	Total	19	100.0	

Table 4.1: Frequency distribution of the banks category

II. Ethiopian bank's key activities pre and post ITDRP deployment

Under this part of the survey there were multiple questions that rise many issues about the banks practices on ITDRP. The main questions were more about tasks before actual plan and post plan action to keep the ITDRP plan up to-date in order to meet the business requirements.

1) Conducting Business Impact Analysis in the banks

Question: Does your bank have experience of conducting business impact analysis?

BIA is the core point of ITDRP which focuses on identifying critical business functions and operations that need to be recovered on priority bases and establish appropriate recovery objective. It should be completed in advance of risk assessment in order to identify urgent functions up on which risk assessment should be focused. Pervious researchers on ITDRP highlighted that, every bank shall conduct institution-wide BIA to identify business functions that are mission critical and potential losses in case of disruption. According this survey all the banks of Ethiopia have experience on conducting BIA for their mission critical services. Some of the banks did not have a comprehensive ITDRP in place but they have the experience of conducting BIA on their mission critical functions regularly.

2) Conducting IT Risk Assessment in the banks

Question: Does your bank have experience of conducting risk assessment?

IT risk assessment looks at probability and impact of variety of specific threats that could cause online business interruption [37].It focuses on the critical business functions identified during BIA.

“Every bank or financial institution shall at least once a year, conduct an institution-wide risk assessment in respect of the identified mission critical functions and ascertain potential for major disruptions” [37].

Each bank in Ethiopia has the unit of IT risk assessment, which identify the potential threats and analyses the tradeoff or opportunity cost for mission critical operations. However, eight of the total banks still have no any comprehensive recovery strategy to face the different potential threats.

3) The presence of IT DRP in Ethiopian banks

Question: Does your bank have an IT Disaster Recovery Plan in place?

Now a day Banks are highly susceptible to operational disruptions caused by internal and external threats such as fire, earth quick, civil unrest, terrorist attacks, system failure, etc. “Such disasters may lead to severe operational disruptions and sometimes threaten the solvency and business continuity of institutions, which could adversely impact the financial system as a whole” [37].

In Ethiopian modern banking history there were not seen any serious threats that disturb the business operations except power outage, network instability and civil unrest which can cause little bite impact on the bank services and their loyal customers.

So due to these probable disruption of business operations banks ought to have comprehensive ITDRP in place. According this study 42.1% (8) of the Ethiopian banks have ITDRP in place but 57.9 % (11) of the banks are on the way of developing the plan, mean the plan is not in practice until the study took place. The 57.9% of banks have not deployed ITDRP so far as the top managers of the banks didn't consider it as urgent, lack of skillful man power and considering as waste if they invest on it because they thought the environment is safe from serious disasters. Though, 42.1% (8) banks have the plan in place but it's far from meeting the international standards setting by the different standards governing body.

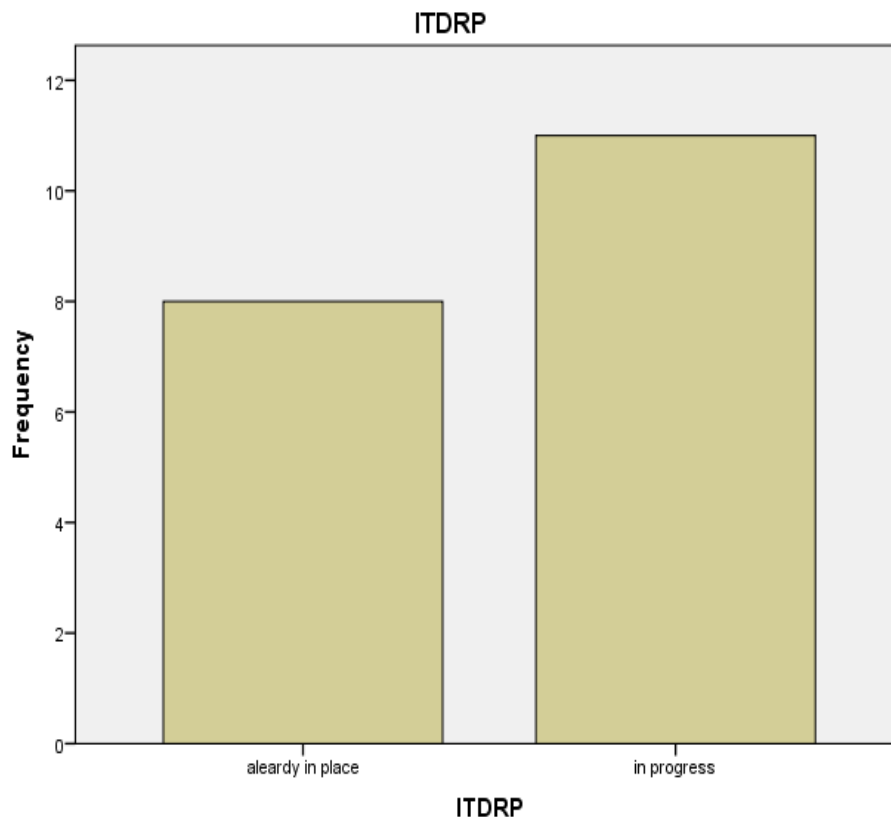


Figure 4.1: Current Status of ITDRP in Ethiopia banks

However, all the banks in Ethiopian have used a daily back up for their critical operations to avoid a minor data loss. And the further responses indicated that the banks are used external

storage devices such disk and magnetic tape for the regular backups and they set specific location where the backed up data can placed.

4) ITDRP Documentation

Question: Is your ITDRP is documented properly?

According the response from banks 63.2% (12) of the banks have documented properly their ITDRP whereas 36.8% (8) of the banks didn't documentation their plan. From 42.1% of the banks which already have ITDRP 75% of the banks have comprehensive documentation of the basic activities and procedures of their plan, but 25% they don't have documented their plan yet. And from 57.9% of the bank which are in progress state 54.5% have prepared their plan before the actual plan implementation and 45.5% they don't have the documentation as the plan is in progress state. Table 4.2 below shows the percentage distribution among ITDRP and plan documentation.

			Documentation		Total
			no	Yes	
ITDRP	already in place	Count	2	6	8
		% within ITDRP	25.0%	75.0%	100.0%
		% within Documentation	28.6%	50.0%	42.1%
		% of Total	10.5%	31.6%	42.1%
	in progress	Count	5	6	11
		% within ITDRP	45.5%	54.5%	100.0%
		% within Documentation	71.4%	50.0%	57.9%
		% of Total	26.3%	31.6%	57.9%
Total	Count	7	12	19	
	% within ITDRP	36.8%	63.2%	100.0%	
	% within Documentation	100.0%	100.0%	100.0%	
	% of Total	36.8%	63.2%	100.0%	

Table 4.2: ITDRP * Documentation Cross tabulation

5) Strategic plan

Question: Is your ITDRP incorporated in the overall strategic plan of your bank?

Response from the 19 banks indicated that 68.1% (13) of the banks have working the plan in align with strategic plan of the banks however 31.9 % (6) of the banks didn't still align the plan with the bank strategic plan. ITDRP is expected to align with mission critical operations of the banks in order to avoid serious business disruption. Table 4.3 shows the frequency distribution of the banks which incorporated their ITDRP or not to strategic plan of the banks.

		Frequency	Percent	Cumulative Percent
Valid	Yes	13	68.4	100.0
	No	6	31.6	31.6
	Total	19	100.0	

Table 4.3: Frequency distribution of the banks which incorporated the plan
With their strategic plan or not

6) Off-site Location Selection and Availability in the Banks

Question: Have you established an alternative site where data can be stored redundantly to the primary site?

The question under this heading aimed at find out what type of plan site is applying by different banks of Ethiopia. Off-site location is a place where data is placed redundantly to the primary location in order to recover huge data when the primary site is failed to work normally.

Table 4.4 below shows the percentage of banks which have offsite location or not.

		Frequency	Percent	Cumulative Percent
Valid	Already in place	7	36.8	36.8
	In progress	12	63.2	100.0
	Total	19	100.0	

Table 4.4: Frequency distribution of the off-site location among the banks

Among the 19 banks 36.8 % (7) have off site location which is synchronized with primary data center and 63.2% (12) haven't an offsite location where data could place redundantly for the purpose of back up during disaster situations. But it's only one bank which met the minimum distance between the primary and offsite location while the five banks didn't meet the minimum distance. Therefore, from 42.1% (8) of the banks which have placed ITDRP only one bank is used onsite location for its ITDRP. In addition the response indicated 36.8% (7) of the bank thought their offsite data center is fully furnished and 15.8% (3) it's assumed to be fully facilitated in time where as 47.4% (9) the banks' offsite data center is far from fully furnished.

7) ITDRP Working Standards in Ethiopian banks

Question: To which standard is your IT Disaster Recovery Plan bench marked?

According the response we found the banks used different international standards to design their off-site and on-site datacenters. Figure 4.2 below shows 47.4% banks used ISO 27k series, 36.8% mixed standards, 5.3% COBIT&ITIL, 5.3% ISO&COBIT and 5.3% have not selected any specific standard yet. Even though the banks are trying to apply the international standards, but they are still fails to meet the standards. For example, most of the bank are not selecting the off-site location based on the standards knowledge, they only consider telecom infrastructures expenditure and they ruled out the possibility of heavy disasters strike. As I discussed in the earlier heading the banks which have ITDRP are using the same location for both data centers which is not meet the standard distance between the two data centers.

Therefore, such limitation could cause serious damage to their critical services during catastrophic situations. However, most of the banks works to meet the directions and rules set by NBE.

Figure 4.2 below shows the percentage distribution of the IT standards used among the Ethiopian banks.

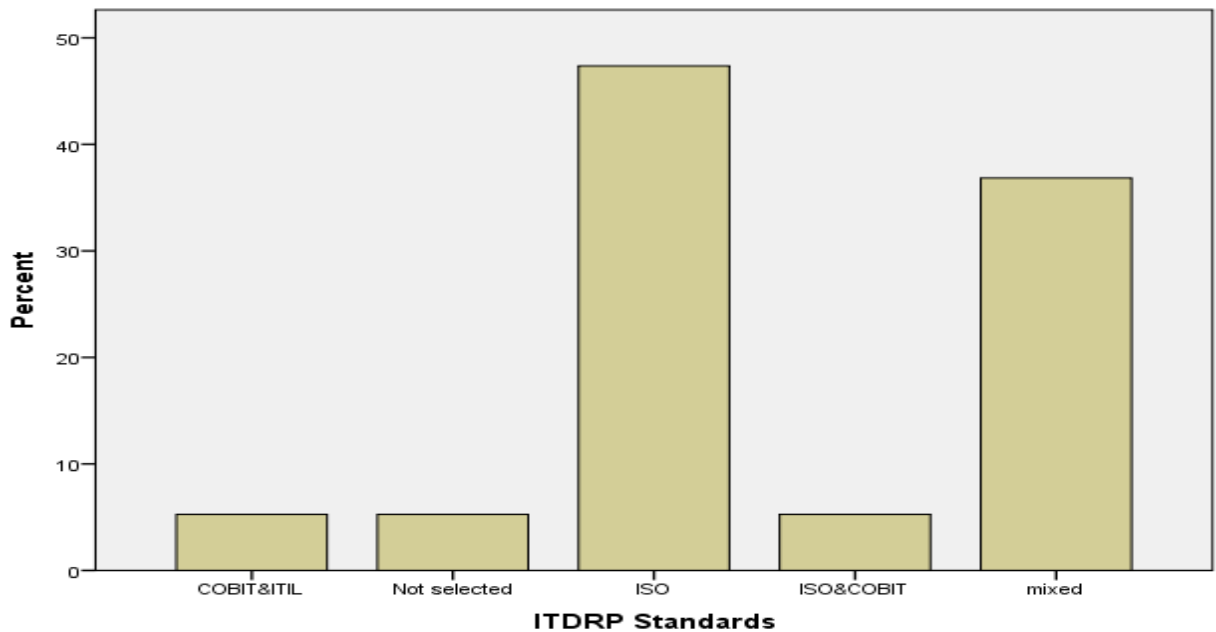


Figure 4.2: Frequency distribution of ITDRP standards usage in Ethiopian banks

8) Recovery Capability of ITDRPs

Question: How quickly can you resume following a disaster?

The question under this heading is aimed to find out how the banks resume their normal operation after disaster strike. Even though the banks have not experienced severe disaster, but they have set the maximum tolerable down time. Banks in Ethiopia which have ITDRP and banks in progress status have tried to give their responses to the above question. Accordingly, the responses range is quite different and even some of the banks didn't put exactly time how fast the system can resume following disaster. Table 4.5 below shows the frequency distribution of the banks RTO. Accordingly, 57.9% (11) of the banks assume they can resume to normal operation with one week time interval, whereas 5.3% immediately (1), 31.6% (6) in hours and 5.3% (1) is not set yet.

		Frequency	Percent	Cumulative Percent
Valid	1 Week	11	57.9	57.9
	Immediately	1	5.3	63.2
	In Hours	6	31.6	94.7
	Not Set	1	5.3	100.0
	Total	19	100.0	

Table 4.5: Frequency distribution of ITDRP recovery capability among the banks

Researchers highlighted that during normal operation there is usually some gap between the last backup performed and the current state of the data [12] [15]. Recovery time in some operations it may be is minutes or hours; in most organizations its' hours or days.

III. Review of ITDRP

9) Testing and Reviewing the ITDRP

Question: How often do you review and test your IT Disaster Recovery Plan?

The question under this heading was aimed to find out how often plan is reviewing. Nature of threats always varies from time to time, so the ITDRP needs to test and update regularly in order to meet what the business needs. Table 4.6 below shows banks have experienced different testing schedule. According the response, 42.1%(8) of the banks tests their plan on annually basis which is familiar the supervision given by NBE, while 5.3% (1) tests depending on situation, 5.3% (1) tests every month, 10.5% (2) not decided yet because the documentation is not finalizing, 5.3%(1) is on pending, 15.8% (3) tests every six months and 15.8% (3) are tests every three month.

ITDRP Testing					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Annually	8	42.1	42.1	42.1
	Depend on situations	1	5.3	5.3	47.4
	Every Month	1	5.3	5.3	52.6
	Not Set	2	10.5	10.5	63.2
	Pending	1	5.3	5.3	68.4
	Six Months	3	15.8	15.8	84.2
	Three Months	3	15.8	15.8	100.0
	Total	19	100.0	100.0	

Table 4.6: Frequency distribution of ITDRP testing among the banks

Though previous researcher indicated that, IT DRP should be tested on annual or after major changes to the technical environment [24].

The central bank of Ethiopian establishes rules and regulations including the reviewing and testing of the plan for the whole banks. Due to that most of the banks review and update their plan on annually basis regardless the environmental and technological changes.

Figure 4.3 depicts the frequency distribution among the banks in Ethiopia how often the plan is reviewed.

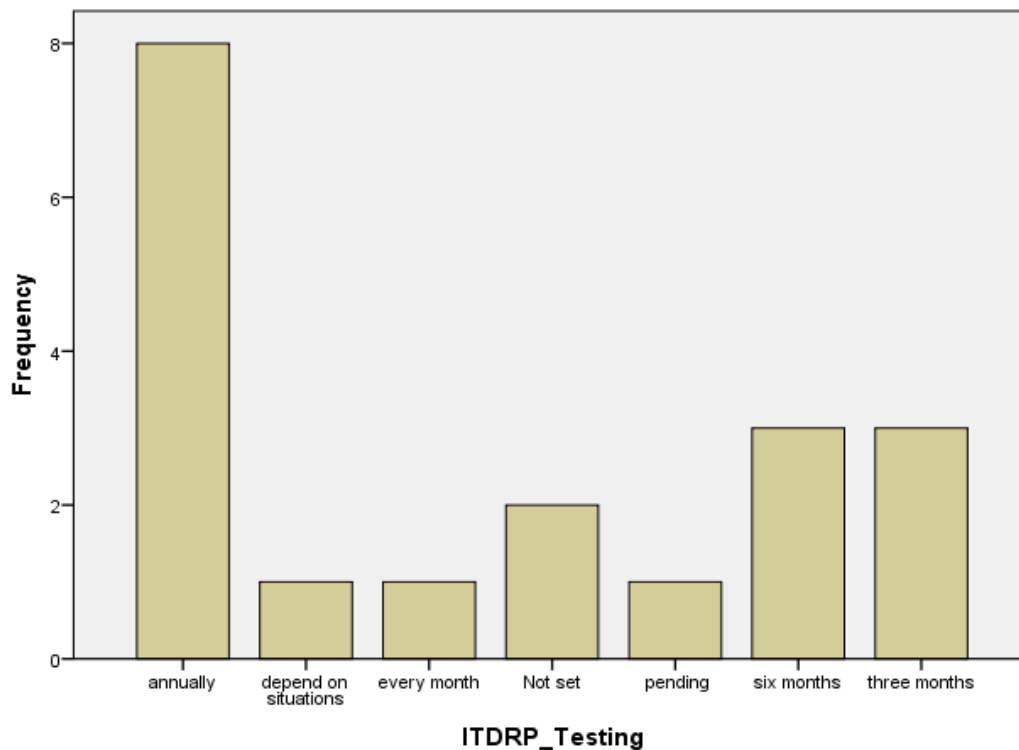


Figure 4.3: Frequency distribution of ITDRP testing experience among the banks

10) Type of testing ITDRP

Question: What type of test do you subject your IT Disaster Recovery Plan to?

Table 4.7 below shows which type of testing approaches did the banks applied. According the responses from the banks, 42.1% (8) of the banks used full simulation testing, 21.1% (21) not decided testing type, and 5.3% (1) used integrated simulation, 21.1% (21) used isolated simulation, 5.3% (1) used table top and 5.3% (1) used walkthrough testing. But this not mean all the banks have ITDRP in place because from earlier discussions it indicated that only 42.1 % (8) of the bank has the plan in work. Though as the 57.9 % (11) of the banks ITDRP is in progress they had the chance to respond the question from the progress they had. ITDRP is never complete, the plan must tested and update at least once per year, if not more frequently [38].

		Frequency	Percent	Cumulative Percent
Valid	Full Simulation	8	42.1	42.1
	No Testing	4	21.1	63.2
	Integrated Simulation	1	5.3	68.4
	Isolated Simulation	4	21.1	89.5
	Table Top	1	5.3	94.7
	Walkthrough	1	5.3	100.0
	Total	19	100.0	

Table 4.7: Type of testing response frequency and percentage distribution

11) ITDRP Auditing

Question: Is your IT Disaster Recovery Plan subjected to the audit process?

The question under this heading was aimed to find out the ITDRP auditing experience of banks in Ethiopia. According the responses received from the respondents, 52.6% (10) of the banks have planned to audit their ITDRPs onwards while 47.4% (9) of the banks don't considered it yet.

Table 4.8 below shows the ITDRP auditing responses frequency distribution among the banks.

ITDRP Auditing					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	9	47.4	47.4	47.4
	Yes	10	52.6	52.6	100.0
	Total	19	100.0	100.0	

Table 4.8: ITDRP auditing responses frequency and percentage distribution

12) Types of IT DRP Auditing

Question: please indicate how often the plan is audited?

The question under this heading is aimed to find out the types ITDRP auditing approach used by the banks in Ethiopia. Table 4.9 below shows the types of ITDRP auditing approaches frequency distribution among the banks. Therefore, responses from the banks indicated that 26.3 % (5) of the banks are planning to audit annually, 36.8% (7) of the banks are on the way to introduce ITDRP auditing, 5.3 % (1) bank has not any idea about IT auditing yet, 10.5 % (2) of the banks plan to audit their ITDRP every six months and 21.1 % (4) every three months.

Type of IT-DRP Auditing					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Annually	5	26.3	26.3	26.3
	in progress	7	36.8	36.8	63.2
	No	1	5.3	5.3	68.4
	six months	2	10.5	10.5	78.9
	three months	4	21.1	21.1	100.0
	Total	19	100.0	100.0	

Table 4.9: Type of ITDRP auditing frequency distribution among the banks

“Every bank or financial institution shall test their ITDRP for effectiveness and update on regular basis. An internal auditor or other independent party shall review the BCP to ensure that it is realistic, reliable, and relevant” [37].

13) ITDRP Effectiveness in Ethiopian Banks

Question: Do you think the plan is adequate and effective enough to ensure that critical operations of the bank are resumed as quickly as possible in an event of disaster?

The question under this heading was aimed to find out how the plan is effective during and after catastrophic situations.

Business continuity management is a whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely

fashion in the event of a disruption. Its purpose is to minimize the operational, financial, legal, and reputational and other material consequences arising from disruption. Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which affords financial industry participants and financial authorities greater flexibility to address a broad range of disruptions. At the same time, however, organizations cannot ignore the nature of the risks to which they are exposed. For example, organizations located in earthquake-prone regions commonly plan for the impact of earthquake-related major operational disruptions” [39]. As the ITDRP focus is to restore the operability of the systems that support critical business operation, so that the organization can return to normal mode of operation as soon as possible, thus minimizing the damage.

Even though the banks in Ethiopia haven’t experienced huge disaster strike; the researchers found that 57.9 %(11) of the banks they believed that the plan is effective in its purpose; whereas 42.1 %(8) of the bank they didn’t think it’s fully effective during sever disaster strike because the banks ponder that plan needs a major improvements to be more effective regardless the environment factors.

		Frequency	Percent	Cumulative Percent
Valid	no	8	42.1	42.1
	yes	11	57.9	100.0
	Total	19	100.0	

Table 4.10.ITDRP effectiveness frequency distribution among Ethiopian banks

IV. ITDRP Team management

14) IT Disaster Recovery Team Management

Question #1: Does your bank have disaster avoidance and recovery committee?

The question under this heading targeted to find out how the banks manage the ITDRP activities during and after the data recovery processes.

Formalizing the roles and responsibilities of the key stake holder through each level of the banks is critical component to achieve effective IT DR. According the response, 21.1 % (4) of the total banks have IT DR committee that works independently whereas 78.9 % (15) of the banks they don’t have IT DR committee that works specifically on it. However, they assumed that all the IT staffs have responsibility before and during the recovery processes

Question #2: Does your bank have clearly assign the roles and responsibilities in ITDR?

The responses for this questions showed that 52.6 % (10) of the banks have clearly assign the roles and responsibilities to IT professionals in the banks while 47.4 % (9) have not assign the role and responsibilities to individuals.

Question #3: Have your employees participated in an emergency preparedness workshop?

This question was aimed to find out how the bank employees prepared in advance regarding emergency preparedness. The response shows that 26.3% (5) of the banks has an experience on preparing short trainings and workshops for their employees whereas 73.7% (14) of the banks haven't prepared any training or workshop regarding emergency preparedness so far.

V. Financial management of ITDRP

15) IT DRP Financial Management

Question #1: Does the board allocate enough budget for Disaster recovery plan?

The question under the heading focused to find out how the ITDRPs are supported by financial imposed by the top management and major stake holders. Responses from the banks shows that 84.2%(16) of the banks top managers have given high attention to the plan and they allocate enough budget, whereas 15.8% (3) didn't consider it as urgent issue and they aren't voluntary to spend big money on it.

Question #2: please indicate how often budget is revised?

Table 4.11 below shows 73.7% (14) of the banks revise their IT DR budget annually, 5.3 % (1) revise every six months, 5.3% (1) revise based on Information System Development (ISD) recommendations and 15.8 % (3) of the banks already indicated that they don't thought it needs special budget allocation.

		Frequency	Percent	Cumulative Percent
Valid	Annually	14	73.7	73.7
	based on ISD recommendation	1	5.3	78.9
	Not	3	15.8	94.7
	six months	1	5.3	100.0
	Total	19	100.0	

Table 4.11 ITDRP budget revision frequency distribution among the banks

4.2.2. Findings from the Qualitative Data

As the questionnaire contains both close ended and open ended questions this analysis focuses on analyzing the open ended responses. Therefore, this section used to validate the quantitative findings by providing further explanations to the quantitative results.

The questionnaire contains open ended questions which respondents have to put their justifications. The first two open ended questions were about the experience of the banks on conducting RA & BIA and almost all the banks responded that they have the experience of conducting RA continuously in order to identify potential threats and vulnerability of their organizations. In addition to the above, most of the banks responded that their banks have custom of conducting BIA with related to the specific applications of the bank in order to predict the consequence of these applications interruption. Results from the qualitative analysis supports the major findings of the quantitative analysis. The quantitative finding indicated that 57.9 %(11) of the banks in Ethiopia are not have ITDRP in place. Accordingly the responses from the qualitative data, the reason of most of the banks is because the plan is under construction and it's not finalized yet.

And some of the banks indicated that the delay of the plan is because of less effort from top managements and unwilling to invest more on it. The 31.9 % (6) of the banks respond that their ITDRP is not incorporated with the strategic plan of the banks. The reasons from the qualitative responses indicated that, this due to the concept of ITDRP is not matured enough to practice. And some banks also indicated that the strategic plan is more focused on improving performance of the system and other security issues.

The 36.8 % (7) of the banks haven't documented their plan so far including two banks which have the plan in place. The findings from most of the banks respondent indicated that the ITDRP is in progress status and document is not finalized yet.

From the 42.1 % (8) of banks which the plan on work, one bank has deployed on-site ITDR rather than off-site. Further finding shows it's only one bank that selected better off-site location which is near to world standards and practices while the rest seven banks used close location to the primary site which is risky in emergency situation [15].

The 42.1% (8) of the banks didn't expect the ITDRP to completely effective. Most of the banks reasoned out that the ITDRP is not fully equipped and the plan needs a major technical enhancements.

For around 47.4% of the banks didn't conduct ITDR auditing; and the finding shows that it's because they don't have IT auditing experience. However, according to directorate of banking supervision of Tanzania, every bank or financial institution shall audit their ITDRP for effectiveness and update on regular basis [37]. An internal auditor or other independent party shall review the ITDRP to ensure that it is realistic, reliable, and relevant.

The 78.9 %(14) from the total banks and 15.8% (3) from the banks with the ITDRP don't have IT DR avoidance and recovery committee; and the finding shows that it's because the plan is not matured and some of the banks thought that the IT department is already responsible for that. And most banks didn't conduct any short trainings and workshops so far for their employees; and this is due to banks didn't consider it as major issue. However, some of the banks responded that they have experienced on conducting workshops in coordinating with some vendors for their employees but they thought it's not sufficient enough.

4.2.3. Discussion

The main objective of the study is to examine the current status of ITDRP in Ethiopian banks. ITDRP are widely accepted as a way to ensure all critical data, IT systems and networks can be recovered in any event of calamity. Now-a-days business contingency has become compulsory for any business organizations to get competitive edge over their competitors. This study revealed that almost all Ethiopian banks are experienced on conducting RA and BIA in order to identify the threats and vulnerability of their business contingency in associate with their mission-critical services. In this study, 57.9 % of the banks are replied that the plan is in place, while 42.1% of the banks didn't put in to work yet. Nevertheless, preceding literatures mentioned that having appropriate recovery strategy in place is not an option for financial institutions. Related work in Zambia identified that all the banks in Zambia are working with the plan, however there is still misunderstanding between ITDRP, BCP and risk management and awareness of the employees regarding the plan [27]. Regarding on the plan documentation routine, 63.2% of the banks have properly documented their plan, whereas, 36.8% of the banks respond that plan documentation is not finalized yet. Preparing a comprehensive documentation of the plan would be helpful during prevention, recovery process and maintenance of the actual plan. Regarding to the strategic plan, six of the banks didn't align their IT-DRP with the strategic plan of the banks. There is a need for commercial institutions to deploy more all-inclusive method to BCP and its relevance to strategic plan and operational aspect of the organization [28]. If the plan is not on strategic level it can't deals with level of risks, and plan wouldn't be practical or achievable within the organization's constraints such as manpower, and budget. For around 36.8% of the banks responded that they have offsite location where data can be placed redundantly to the primary site in order to recover after interruption occurrence. However, the deployment of the secondary location is not well reinforced using international practices and guidelines. As per the study in Sri Lanka, the delineation about alternative site is not adequate when considering the current competitive business environment [4].Directly the above study suggested that the banks should have a hot site as disaster recovery site. According to NIST thoughtful, the location of the primary and secondary site should be determined on the basis of potential threats and not merely by the distance between them [40]. According the responses from the banks, the effectiveness of the plan is questionable and the maximum tolerable downtime is not calculated based on scientific manner. Therefore, the values for RTO &RPO were fathomed by the relevant experts without estimating the real values.

This study reveals that the IT-DRP testing methods of the banks are varied from one bank to other bank. Most of the banks test their plan on annual basis which is related to the compliance of the central bank of Ethiopia. Though, IT-DRP should be tests on annual basis or after major update to the technical environment [4]. Normally, as the IT-DRP practice is not matured enough in Ethiopian banks the subsequent activities such as reviewing and auditing of the plan are not handling properly.

4.2.4. Chapter summary

This chapter presents the data analysis results and its interpretation from the self-administered questionnaire which is contained both close-ended and open-ended questions. The results were presented in simple descriptive statistics format such frequency, percentage, and charts. Findings of this study indicated that some of Ethiopian banks have properly deployed ITDRP in place in order to limit data loss during devastating circumstances. However, most of banks in Ethiopia are not placed in an all-inclusive ITDRP yet. Generally, the findings of this study directed that ITDRP practices is not matured enough across the financial institutions of Ethiopia.

Chapter Five

Conclusion and Recommendation

5. Introduction

This chapter presents the conclusion drawn from the major findings, practical implications of the findings, recommendations forwarded, and possible future works in the area. The conclusion and recommendation forwarded were focused on addressing the objective of the study. The limitation of the study is also discussed with the future works of the study.

5.1. Conclusion

The research reported in this paper attempts to understand the current status of the ITDRP Ethiopian banks. The objective of the study was to investigate the ITDRP experience in Ethiopian banks. As we all know that bank's data are very important and crucial, the loss may lead to entire business failure and it could affect the economy of the country and individuals as well. Due to advancement of IT, banks and other financial institutions nowadays heavily depends on IT. With emergency of e-business many banks can't even survive without operating 24 hours per day and seven days a week. Accordingly, now-a-days ITDRP is not an option for the banking sector because a reliable IT services have become integral part of most business organizations.

From the results and findings of the primary data analysis the following conclusion were drawn:

- Most of the banks in Ethiopia don't have the ITDRP in place and this is because of the top management didn't look it as serious issue and un willing to invest more on it and lack sever disaster strike experience so far.
- Most of those banks who have the plan use an off-site location too close to the primary site which cannot meet the international standard of minimum distance.
- Most of the banks are forced to select Addis Ababa as their off-site location because of Ethio Telecom high capacity network infrastructure costs too much to extend beyond Addis Ababa.
- Most of the ITDRP needs a major technical improvement since it's deployed with limited resources.
- The testing and updating plan of the banks is more subjected to the norm of the central bank.

- IT auditing ritual is very weak in most of the bank.

5.2. Practical implication of the study

The finding of study shows that most of the banks in Ethiopia have lack of ITDRP practice despite low disaster exposure. However, top managers and major stakeholders should consider ITDRP as main part of BC to avoid Single Point of Failure (SPF); because the lack of disaster strike so far can't be a guarantee for the future survival of the business. A proper implementation of all-inclusive ITDRP can help banks to keep available their mission critical services for 24 hours and this may help them to attract new customers and keep the loyal customers. Generally, this study could motivate the banks to improve the traditional IT disaster recovery strategy and apply all the renowned guidelines during development and maintenance of the plan.

5.3. Recommendation

The intention of this research is to motivate top manager of the banks to take action despite the different challenges. As the finding from the primary showed that most of the banks in Ethiopia haven't a comprehensive ITDRP in place to prevent system disruption in case of disastrous condition. And 42.1% of the banks thought that they have the plan in work but most of the plans are not developed following the international standards and guidelines and it's not sufficient enough to keep the business going on during and after large scale disaster. Consequently, based on the conclusion of the study, the following recommendations are made in two parts which goes to the banks who haven't the plan in place and the banks working with it.

For the banks which haven't the plan at all:-

- The banks should conduct BIA and RA continuously to identify the mission-critical operations of their business, possible environmental threats and the potential risks of the mission critical functions interruption.
- There is need for the banks to adopt a more holistic approach to ITDRP and its relevance to strategic and operational aspect of their organizations
- The banks must incorporate the ITDRP with corporate strategy of the banks. Because this approach will ensure adequate resources allocation to ITDRP.
- The banks should select off-site location based on the international guidelines such as ISO, IBM and COBIT/ITIL. For example the location for the off-site and on-site datacenter should be safe from environmental risk factors like earth quake, flooding, fire etc. And the distance between the primary site and offsite location should be far as much as possible to avoid total damage of both datacenters.

For the banks which have the plan in place:-

As the finding showed that 42.1% of banks have the ITDRP in place but there are a still lot of works the banks should do regarding the plan. And the following are the major recommendations made regarding the major tasks of the plan during development process and after the implementation.

- The banks should follow at least one of the following worldwide standards such as ISO/IEC 27K series, NIST and COBIT/ITIL during implementation and post implementation of the plan. However, there are also national wise standards to be used for ITDRP implementation such as BS25999 for British Standard and RBI for Indian standard.
- Environmental risk factors should not be totally ignored by the banks. Therefore, they should be ready to face any disastrous situations by deploying comprehensive ITDRP in place.
- The location for the IT DR site should be selected on technical manner
- As the type of threats are varying from time to time the plan should be tested, updated and audited regularly in order to meet the business needs.

5.4. Limitations and Future works of the study

Although the findings of this research is based on the primary data gathered from the IT directors of each bank, findings of this study can't be generalized to the other financial institutions. This study has successfully examined the current status of ITDRP practice in Ethiopian banks.

Therefore, based on the findings of this research the following issues can be researched in further study:-

- This work could be further studied using all financial institutions without restricting to the bank sector. Financial institutions can be researched in further study includes insurances, micro finances, etc.
- Now as the banks which have the plan is clearly identified, the next researchers could extended this work on the routine activities of the plan during prevention and recovery strategies process using standard check lists.
- The finding of this research indicated there is lack of exercising of ITDRP adoption in most of Ethiopian banks, therefore next researchers can research on ITDRP adoption
- And some of the findings of this study indicated that some of the bank's top manager thought ITDRP is not thoughtful issue. Thus, this study could be further extended regarding the perception of top managers

References

- [1] S. Goswami, D. A. K. V. and D. S. Garg, "An Introduction and Necessitate of Business Continuity Plans," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 11, pp. 337-340, 2012.
- [2] C. Kadlec and J. Shropshire, "Best Practices in IT Disaster Recovery Planning Among US Banks," *Journal of Internet Banking and Commerce*, vol. 15, no. 1, pp. 1-11, 2010.
- [3] C.-L. Yang, B. J. C. Yuan and C.-Y. Huang, "Key Determinant Derivations for Information Technology Disaster Recovery Site Selection by the Multi-Criterion Decision Making Method," *Sustainability*, vol. 7, pp. 6149-6188, 2015.
- [4] M. Uddin, S. Hapugoda and R. Chand Hindu, "Disaster Recovery Framework for Commercial Banks in Sri Lanka," *J. ICT Res*, vol. 9, no. 3, pp. 263-287, 2015.
- [5] SAN, "Disaster Recovery Plan Strategies and Processes," 2002.
- [6] NBE, "History of Ethiopian Banking," Insurance, Banking and Negotiable Instrument Law, Addis Ababa, 2012.
- [7] C. Bahan, "The Disaster Recovery Plan," SANS, 2003.
- [8] H. A. R. Mohamed, "A Proposed Model for IT Disaster Recovery Plan," *I.J. Modern Education and Computer Science*, vol. 4, pp. 57-67, 2014.
- [9] S. Maitra, D. M. Shanker and P. K. Mudholkar, "Business Continuity and Disaster Recovery Experience in Indian Banks," *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, vol. 2, no. 4, pp. 526-534, 2013.
- [10] J. Shropshire, "Developing the IT Disaster Recovery Planning Construct," *Journal of Information Technology Management*, vol. xx, no. 4, pp. 37-56, 2009.
- [11] plante; Moran, "Business Continuity Planning," Plante & Moran, PLLC, 2017.
- [12] Susan Snedaker, *Business Continuity & Disaster Recovery*, Burlington: Syngress Publishing, Inc., Elsevier, Inc., 2007.
- [13] R. Choudhary and D. (. K. Bhattacharya, "Business Continuity Planning: A Study of Frameworks, Standards and Guidelines for Banks IT Services," *International Journal of Emerging Research in Management & Technology*, vol. 5, no. 8, pp. 33-40, 2016.

- [14] Storkey, "Operational Risk Management and Business Continuity Planning for Modern State Treasuries," 2011.
- [15] IBM, Disaster Recovery Strategies with Tivoli Storage, North Castle Drive Armonk, NY 10504-1785 U.S.A.: IBM Corporation,, 2002.
- [16] ISO27001, "Roles and responsibilities for contingency planning," ISO, 2008.
- [17] Reeder, "Building and Maintaining a Business Continuity Program," Intel, Santa Clara, 2016.
- [18] Xie Qiuyin and Michelle, "Portfolio-Based Approach for Disaster Recovery Planning for IT," in *11th Pacific-Asia Conference on Information Systems*, Singapore, 2012.
- [19] WorldBank, "FINANCIAL PROTECTION AGAINST NATURAL DISASTERS," Worldbank, Washington DC 20433, 2014.
- [20] L. L. Hoong and G. Marthandan, "Critical Dimensions of Disaster Recovery Planning," *International Journal of Business and Management*, vol. 9, no. 14, pp. 145-158, 2014.
- [21] NASA, "The 4th International Workshop on Independent Verification & Validation of Software," University Chennai, Mailam, 2012.
- [22] Queensland, "Business continuity planning," The State of Queensland, 2009.
- [23] W. Krockner, "Disaster Recovery Plan Testing: Cycle the Plan,Plan the Cycle," SANS Institute, 2017.
- [24] F. U. "IT Disaster Recovery Framework," Flinders University, 2013.
- [25] V. Svata, "System View of Business Continuity Management," *Journal of Systems Integration*, vol. 2, pp. 19-35, 2013.
- [26] M. M. Kozina, "COBIT - ITIL mapping for Business Process Continuity Managemen," in *Central European Conference*, Varaždin, 2009.
- [27] M. Simwayi, "An Investigation into the Effectiveness of Business Continuity Plans for Commercial Banks in Zambia," University of the Free State, 2008.
- [28] M. Hınca, "Business continuity and disaster recovery for IS," 2006.

- [29] T. P. S. B. D. Sharma and S. S. K. , "Disaster Recovery and Business Continuity Planning for Electronic Banking: A Comparative Study," *International Journal of Commerce and Management*, vol. 9, pp. 64-71, 2015.
- [30] W. Carrie, "Research Methods," *Journal of Business & Economic Research*, pp. 65-72, 2007.
- [31] G. Abebe, "The Impact of Information and Communication Technology on Performance of Commercial Banks in Ethiopia," AAU, Addis, 2016.
- [32] J. w. Creswell, Research Design, 4 ed., K. Vicki , Ed., Los Angeles, California: SAGE Publications, Inc., 2014.
- [33] S. N. Hesse-Biber, Mixed Methods Reseach, New York: THE GUILFORD PRESS, 2010.
- [34] M. Zohrabi, "Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings," *Theory and Practice in Language Studies*, vol. 3, no. 2, pp. 254-262, 2013.
- [35] C. L. Kimberlin and A. G. Winterstein, "Validity and reliability of measurement instruments used in research," *Am J Health-Syst Pharm*, vol. 65, pp. 2276-2288, 2008.
- [36] A. Bryman and E. Bell, Business Research Methods, 2nd edition ed., Oxford University Press, 2007.
- [37] Bank of Tanzania, "Business continuity management guidelines for banks and financial institutions," Bank of Tanzania, 2009.
- [38] N. Chip, "A Frame Work for Disaster Recovery Planner," in *Comprehensive Consulting Solution, Inc.*, USA, 2008.
- [39] Supervision Basel Committee on Banking, "High-level principles for business continuity," Bank for International Settlements, Swizerland, 2005.
- [40] J. D. Arden L. Bement, Contingency Planning Guide for Information Technology Systems, Elizabeth Lennon, Ed., Washington, USA: NIST, 2002.
- [41] Shaikh, "Ethiopian banker's perception of electronic banking in ethiopia: A case of Adama city," *Internationa journal of scientific and resaerch publications*, vol. 4, no. 9, pp. 1-7, 2014.
- [42] S. Kevin , "Analyzing and Interpreting Mixed Methods Research," Temple University, 2014.

APPENDICES

Appendix A: Letter of cooperation written by the university to the banks.

የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት



College of Natural Science
School of Information
Science

Date February 16, 2017

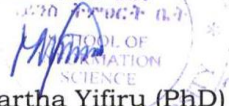
Ref: -SIS/38/2017

To Whom It May Concern

Student Haylay Gebrezgabher (ID.No. GSR/0925/08) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "Investigation of Disaster Recovery Plan in Ethiopian Banking Sector".

I would like to thank you in advance for all the assistance that you would provide to the student.

With Regards,


Martha Yifiru (PhD)
Head, School of Information Science

☒: 1176

☎: +251-(11)-122-91-91 ☎: 2122- 91-92

Appendix B: Survey Questionnaire

Questionnaire on the current Status of IT Disaster Recovery Plan in Ethiopian Banking Sector

Date: 07/03/2017

To: _____

Dear Sirs,

My name is Haylay Gereziher and I'm a post graduate student at the School of Information Science, Addis Ababa University. For my master's thesis, I am investigating the current status of IT disaster recovery planning in Ethiopian banking sector. IT disaster recovery plan is one of the core components of business continuity management used to prevent business interruption during and after fatal disasters. IT disaster recovery plan is a must for banks to keep their mission critical operations alive during and after disastrous conditions. As such the banking sector of Ethiopia is the focus of my study.

As you are one of the major bank in Ethiopia, I hope that the IT department of your bank would participate in this study by completing the attached questionnaire prepared for studying IT disaster recovery plan in Ethiopian banks. The questionnaire will require approximately half of an hour to complete. I would like to assure you that your responses will be kept completely confidential.

I would appreciate your cooperation in completing the questionnaire in 10 days after receiving it. I will come to your office to collect the completed questionnaire. If you require additional information or have questions on the questionnaire, please contact me at the following number: 092-023-3352.

Thank you for taking your time to complete the questionnaire.

Sincerely,

Haylay G/egabher

IT Disaster Recovery Planning Questionnaire

Kindly supply the following information regarding your organization by indicating with an “x” in an appropriate box or writing the answer in the space provided.

SECTION I. INSTITUTIONAL DATA

1. What is the name of your Bank? _____
2. What position do you currently hold? _____
3. In which category does your Bank fall?

Private bank	
State-owned bank	

SECTION II. IT DISASTER RECOVERY PLAN (ITDRP)

4. Do your bank have an experience of conducting Business Impact Analysis(BIA)?(Yes/No)
5. Do your bank have an experience on conducting Risk Assessment (RA)?(Yes/No)
6. Does your bank have back up system for information & records? (Yes/No)
7. If your answer is “NO” for question 6 above, please give the reasons.

8. Does your bank have an IT Disaster Recovery Plan (ITDRP)?

Not started	
In progress	
Already in place	

9. If your answer for question 8 above is “NOT STARTED”, please give the reasons why your bank doesn’t have the plan in place?

10. Is your Disaster Recovery Plan policies and procedures documented properly?

Yes	
No	

11. If your answer is "NO" for question 10 above, please give the reasons.

12. Is your Disaster Recovery Plan incorporated in the overall strategic plan of your Bank?

Yes	
No	

13. If your answer is "NO" for question 12 above, please give the reasons below.

14. Have you established an alternate location (off-site) where data can be placed redundantly to the primary site?

Already in work	
In progress	
No	

15. If your answer is "NO" for question 14 above, please give the reasons.

16. How quickly can you resume to usual operation following a disaster strike?

1Week ☐ 2Weeks ☐ 3Weeks ☐ Longer ☐

SECTION III. REVIEW OF DISASTER RECOVERY PLANNING

17. How often do you review and test your IT Disaster Recovery Plan?

Annually	
Every 6 months	
Every 3 months	
Every month	
Others please specify	

18. What type of test do you subject your IT Disaster Recovery Plan to?

Table top: testing the accuracy of the plan theoretically	
Walk through: step by step testing	
Integrated simulation: live activation of the plans	
Isolated simulation: Testing specific application in association with the hardware	
Full simulation: testing all critical applications	
Others please specify	

19. Is your IT Disaster Recovery Plan subjected to the audit process?(**Yes/No**)

20. If your answer is “YES” for question 19 above, please indicate how often the plan is audited?

Annually	
Every 6 months	
Every 3 months	
Every month	
Others please specify	

21. If your answer is “NO” for question 21above, please give the reasons.

22. To which standard is your IT Disaster Recovery Plan benchmarked? Standards include like, ISO, IEC, IT, COBIT, and others (please specify).

23. Do you think the plan is adequate and effective enough to ensure that critical operations of the bank are resumed as quickly as possible in an event of disaster?

Yes	
No	

24. If your answer for question 23 above is “NO”, please give the reasons below.

SECTION IV. IT disaster recovery plan Team management

25. Does your bank have IT disaster avoidance and recovery committee?

Yes	
No	

26. If your answer for question 25 above is “NO”, please give the reasons below.

27. Have your employees ever participated in an emergency preparedness workshop?

Yes	
No	

28. If your answer for 27 above is “NO”, please give the reasons below.

29. Does your bank have clearly assign the roles and responsibilities in ITDRP?

Yes	
No	

30. If your answer for 29 above is “NO”, Please give the reasons below?

SECTION V. Financial Management for IT Disaster Recovery Plan

31. Does the board voluntary to allocate adequate budget for ITDR purpose?

Yes	
No	

32. If your answer is “yes” for question 31 above, please indicate how often budget is revise

Every 6 months	
Annually	
Others (please specify)	

33. If your answer for question 31 above is” NO”, please give the reasons below.

Thank you for completing the questionnaire!

Appendix C: Letter request for cooperation to IT Infrastructure unit at UNITED BANK S.C



ኢትዮጵያ ባንክ አ.ማ.
UNITED BANK S.C.

Inter office Memorandum

To: Manager, IT Infrastructure & Card Payment
Operation Dep't

From: Manager, HRM Department

A handwritten signature in blue ink, appearing to be 'fms'.

IOM/HRMT/053/17
Date: March 10, 2017

Re: Request for Cooperation

Haylay Gebrezgabher, graduate student of Information Science at the Addis Ababa University is doing his thesis on "Investigation of Disaster Recovery Plan in Ethiopian Banking Sector". And, he wants to approach your Department to collect information through questionnaire.

This is, therefore, to kindly request your usual cooperation in assisting him to get the questionnaire filled out by staff under your domain.

CC

- Ato Haylay Gebrezgabher