ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION TECHNOLOGY DISASTER RECOVERY FRAMEWORK DEVELOPMENT FOR ETHIO-TELECOM

BY: ASEFA ALEMU DEGEFA

OCTOBER, 2020

ADDIS ABABA ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION TECHNOLOGY DISASTER RECOVERY FRAMEWORK DEVELOPMENT FOR ETHIO-TELECOM

A thesis submitted to the College of Natural and Computational Sciences of Addis Ababa University in partial fulfillment of the requirements for the degree of Master of Science in Information Science and Systems (Information Systems Track)

By: Asefa Alemu Degefa

Advisor: Workshet Lamenew (PhD)

October, 2020

Addis Ababa Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION TECHNOLOGY DISASTER RECOVERY FRAMEWORK DEVELOPMENT FOR ETHIO-TELECOM

BY: ASEFA ALEMU DEGEFA

Name and signature of Members of the Examining Board

Workshet Lamenew (PhD)	_____	01/10/2020
Advisor	Signature	Date
Lemma Lessa (PhD)	_____	01/10/2020
Examiner	Signature	Date
Dereje Teferi (PhD)	_____	01/10/2020
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 were acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Asefa Alemu Degefa

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

Advisor's Signature: _____

Workshet Lamenew (PhD)

DEDICATION

This Thesis is dedicated: -

To all Peoples of the world who have dispossessed their lives due to the pandemic **COVID-19**.

To my family.

And above all, to the Almighty GOD.

AKNOWLEDGEMNTS

First, I would like to thank the almighty God for his endless blessing and helping me to finalize this thesis with full of health in this pandemic (COVID-19) time. Then, I would like to express my very special thanks to my advisor **Dr. Workeshet Lamenew** for his tireless encouragement and his academic commitment for guidance.

My dad Ato Alemu Degefa and My Mom W/ro Berhane Gebrekidan who they pay a lot and did a tiring work to make this whole thing possible. Their major work is educating me without getting education for themselves. I really need to say thanks as they are my walking stick always.

Finally, I would be happy if I say thanks to those individuals written their name & description who are part of my success. Nigisti Berhe Gezahegn (my lovely wife and a mother of our children; Michale Asefa and Yohannes Asefa) and her beloved family, Tigist Adane (our household servant), my uncle Haftu Degefa and His Wife Mekbeb Etay, Embafresu Weres (my beloved elder sister), Niguse Alemu (my beloved eldest brother), Hiluf Alemu (my beloved brother), Tsehaye Negash (my school mate and groomsman in my marriage), ethio telecom staffs who were participants of this study and Addis Ababa University whole Community specific to instructors.

Asefa Alemu

October, 2020

TABLE OF CONTENTS

DECLARATION ..... **I**

DEDICATION ..... **II**

AKNOWLEDGEMNTS ..... **III**

TABLE OF CONTENTS ..... **IV**

ABSTRACT ..... **VIII**

LIST OF FIGURES ..... **X**

LIST OF TABLES ..... **XI**

LIST OF ACRONYMS ..... **XII**

CHAPTER ONE **1**

1. INTRODUCTION 1

1.1. BACKGROUND OF THE STUDY 1

1.2. RESEARCH MOTIVATIONS 4

1.3. STATEMENT OF THE PROBLEM 5

1.4. RESEARCH QUESTIONS 6

1.5. OBJECTIVE OF THE STUDY 7

1.5.1. GENERAL OBJECTIVE 7

1.5.2. SPECIFIC OBJECTIVES 7

1.6. SIGNIFICANCE OF THE STUDY 7

1.7. SCOPE (DELIMITATIONS) OF THE STUDY 8

1.8. ORGANIZATIONS OF THE STUDY 8

CHAPTER TWO **10**

2. LITERATURE REVIEW AND FRAMEWORK DEVELOPMENT 10

2.1. CHAPTER INTRODUCTION 10
2.2. DEFINITIONS AND TYPES OF DISASTERS 10
2.3. IT DISASTER 11
2.4. IDENTIFICATION OF IT DISASTERS 12
2.5. IT DISASTER RECOVERY SITE 12
2.6. TYPES OF ITDR SITES 14
2.6.1. HOT SITE 15
2.6.2. WARM SITE 16
2.6.3. COLD SITE 16
2.6.4. MOBILE SITE 17
2.6.5. MIRRORED SITE 17
2.6.6. WINGING SITE 17
2.7. IT DISASTER RECOVERY PLAN 17
2.7.1. ELEMENTS OF IT DISASTER RECOVERY PLAN 20
2.7.2. STRATEGIES OF ITDRP 22
2.7.3. PHASES OF IT DISASTER RECOVERY PLAN DEVELOPMEN 22
2.7.4. ITDRP TESTING TECHNIQUES 24
2.7.5. IMPORTANCE OF IT DISASTER RECOVERY PLAN 25
2.7.6. BEST PRACTICES OF ITDRP SERVICES 27
2.7.7. CHALLENGES INFLUENCING ITDRP IMPLEMENTATION 29
2.8. RELATED WORKS 31
2.9. CONCEPTUAL FRAMEWORK OF ITDRP 42
2.10. ITDR FRAMEWORK DEVELOPMENT FOR ETHIO TELECOM 44
2.11. CHAPTER SUMMARY 47

CHAPTER THREE 49

3. RESEARCH METHODOLOGY 49
3.1. CHAPTER INTRODUCTION 49

3.2. RESEARCH DESIGN 50
3.3. SINGLE CASE STUDY RESEARCH DESIGN 51
3.3.1. UNIT OF ANALYSIS AND UNIT OF OBSERVATION 54
3.3.2. PARTICIPANTS SAMPLING TECHNIQUES 56
3.3.3. CONTRIBUTORS ELIGIBILITY CRITERIA 58
3.3.4. DATA COLLECTION TOOLS AND TECHNIQUES 59
3.3.4.1. DISASTER RECOVERY PLAN LITERATURE REVIEW AND DOCUMENT ANALYSIS 59
3.3.4.2. PROCESS OF SEMI-STRUCTURED INTERVIEWS (SSI) 60
3.4. DATA ORGANIZATION TECHNIQUES 65
3.5. DATA ANALYSIS 66
3.6. RESEARCH QUALITY ASSURANCE 68
3.7. CHAPTER SUMMARY 71

CHAPTER FOUR 73

4. CASE-STUDY ANALYSIS, FINDINGS, DISCUSSION AND SUMMARY OF RESULTS 73

4.1. CHAPTER INTRODUCTION 73
4.2. CASE STUDY ANALYSIS 74
4.3. ITDR GAP INVESTIGATION 75
4.4. AWARENESS OF IMPLENENTING ITDR IN ETHIO TELECOM 77
4.5. CHALLENGES TO ATTAIN ITDRF IN ETHIO TELECOM 78
4.6. LEVEL OF IMPORTANCE HAVING ITDR TO THE COMPANY 79
4.7. IMPLEMENTATION STRATEGIES OF ITDR IN ETHIO TELECOM 81
4.8. REVISING THE FRAMEWORK 84
4.9. TESTING THE FRAMEWORK 85
4.10. DISCUSSION 86

4.11. CHAPTER SUMMARY 87

CHAPTER FIVE 88

5. SUMMARY OF RESULT, CONCLUSIONS, RECOMMENDATIONS AND FUTURE RESEARCHES 88

5.1. CHAPTER INTRODUCTION 88

5.2. SUMMARY OF RESULT 88

5.3. CONCLUSION 89

5.4. LIMITATIONS OF THE STUDY 90

5.5. RECOMMENDATIONS 91

5.6. FUTURE RESEARCH 92

5.7. CHAPTER SUMMARY 93

REFERENCES 94

APPENDIX_A: UNIVERSITY COOPERATIVE LETTER WRITTEN TO CASE COMPANY ETHIO TELECOM 104

APPENDIX_B: SSI OBJECTIVES DECLARATION, SSI PROCEDURES AND SSI QUESTIONS 105

APPENDIX_C: URKUND ANALYSIS REPORT 109

ABSTRACT

Data and infrastructure of telecommunications should be properly managed and protected. If data and infrastructures of a telecom company could not be properly managed there may be loss which hinder the services or which totally destroys even the existence of the organization for some period of time till re installment takes place. Service blackouts and data loss could be created in either natural disasters or deliberate and none-deliberate man-made disasters which results in monetary and infrastructure loss.

This study focused on disaster recovery (DR) practices in telecommunication sector of Ethiopia that is ethio telecom. The objective of this study was to develop a framework of ITDR for ethio-telecom. To realize this objective, the researcher had preliminary study and detail literature review. From the preliminary investigations and semi-structured interviews conducted on the main study of the research showed that ethio tlecom has no ITDR currently, rather it has ad-hoc incident management for services restoration and resolve any service interruptions. The study concluded that ethio telecocm only has ad-hoc DR practices and there was no any internationally accepted and standardized or locally agreed and practicable ITDRF in the company. Data was collected from two sources 1. From departments' document analysis 2. Conducting semi structured interview from 25 respondents. Twenty-five participants were chose from five departments located in two divisions purposefully for a qualitative case study research data collection. Data collected from 20 participants was held face to face semi-structured interview and from 5 participants on phone calls. The data collected related to current status and practice of IDR in ethio telecom was interpreted qualitatively using QDA Miner Lite and theme was grouped and merged as suited as possible for report writing. Based on the existing scholarly works reviewed literature and data collected from document analysis & semi structured interviews this study brought a simplified and manageable customized framework of ITDR for ethio telecom.

The proposed framework was a knowledge extending framework from banking sector to telecom sector with some considerable set-up and operational adaption. The proposed framework was presented for internal experts' validation for its efficiency, effectiveness and worthwhile to the critical functioning areas of ethio telecom. Ten

evaluators were given a testing factors in a separated 2 domains having 20 sub domains. The result given by the experts was 88.12% and showed that the framework is acceptable for telecom sector specifically suitable to ethio telecom with regard to current situations and needs of the company for ITDR framework.

Keywords: Disaster, Disaster Recovery, IT Disaster, IT Disaster Recovery, IT Disaster Recovery Framework, Disaster recovery site, telecom sector, ethio telecom, factors, Business Continuity, implementation, qualitative, case study, pattern matching, explanation building, themes searching, Judging, Validity, reliability

LIST OF FIGURES

Figure 1: Types of Disasters collected from different literatures 11
Figure 2: Illustrates ITDR site using a secured remote access gateway as a bridge between the primary site and DR site (Adapted from Robb, 2019) 13
Figure 3:Shows the RPO, RTO, WRT and MTD (Adapted from Marek, 2013) 15
Figure 4: Core components of business continuity (Adapted from Telecom Excellence Academy, 2017) 18
Figure 5: Interactions of BC/DR elements (reprinted from Snedaker, 2007 p.6) 21
Figure 6: Sample ITDRF set up (Reprinted from Uddin et al., 2015 P. 277) 33
Figure 7: Conceptual ITDRF for ethio telecom (adapted from Uddin et al., 2015) 47
Figure 8: Illustration of holistic and embedded research designs under single case and multiple case (Reprinted from slide share.com) 53
Figure 9: Illustrates single case design (adapted from Solomon, 2018 p.53) strates single case design (adapted from Solomon, 2018 p.53) 54
Figure 10: Classifications of unit of Analysis (Adopted from Kumar, 2018 p.72) 55
Figure 11: Basic sampling methods (Adapted from Sarstedt et al., 2017) 57
Figure 12: Process of semi-structured interview 65
Figure 13: Process of semi-structured data organization 66
Figure 14: Illustrates steps of data analysis employed on this case study research..... 68
Figure 15: The Modified and final developed ITDRF for ethio telecom 85

LIST OF TABLES

Table 1: Motivation and needs for ITDR research compiled from scholarly works.....5
Table 2: Summary of related works from the reviewed literature 41
Table 3: Illustrations of interviewee distribution across their hierarchy.....63
Table 4: Contributors working department, time table and mode of interview.....64
Table 5: Detail research activities done to maintain quality in the study 70
Table 6: Interviewee detailed information 74
Table 7: Modality of semi-structure interviews and their durations.....74
Table 8: Mapping of research questions and specific objectives.....75

LIST OF ACRONYMS

BC - Business Continuity

BIA - Business Impact Analysis

BSS - Base-Station Subsystem

CB - Commercial Banks

CBS - Convergent Billing System

CC - Continuous Computing

CDMA - Code-Division Multiple Access

CEO - Chief Executive Officer

CM - Crisis Management

COBIT - Control Objectives for Information Technology

COVID - 19 - Corona Virus Disease 2019

CRM - Customer Relationship Management

DC - Data Center

DR - Disaster Recovery

DRS - Disaster Recovery Site

EM-DAT - Emergency Events Database

GSM - Global System for Mobile communication

GSMA - Global System for Mobile Communication Association

HIPAA - Health Insurance Portability and Accountability Act

HSS - Home Subscriber Server

IFRCRCS - International Federation of Red Cross and Red Crescent Societies

IPCC - Internet Protocol Call Center

IRBCMS - ICT readiness for support of a broader business continuity management system

ISD - Information Systems Division

ISF - Information Service Functions

ISO/IEC - International Organization for Standardization/International Electro Technical Commission

IT - Information Technology

ITDR – Information Technology Disaster Recovery

ITDRF - Information Technology Disaster Recovery Framework

ITIL - Information Technology Infrastructure Library

ITSC - IT Service Continuity

IoT - Internet of Things

LTE - Long-Term Evolution

MTD - Maximum Tolerable Downtime

NFPA – National Fire Protection Association

NIST - National Institute of Standards and Technology

NSS - Network and Switching Subsystem

PDCA - Plan, Do, Check, Act

PMBOK - Project Management Body of Knowledge

PRINCE2 - Projects IN Controlled Environments

QDA - Qualitative Data Analysis

RA - Risk Assessment

RPO – Recovery Point Objective

RTO -Recovery Time Objectives

SSIs - Semi-structured interviews

WARP - Work Area Recovery Plan

WRT - Work Recovery Time

CHAPTER ONE

1. INTRODUCTION

1.1. BACKGROUND OF THE STUDY

Technology development has enormous role on human civilization. Remembering back to older history the world was not a small village as looks like now. Getting information from somewhere to act based on that information was too difficult. Nowadays, the development of telecommunication and Information Technology (IT) has changed the way. People are now using information for their weather, food, shopping, education, health, agriculture generally for their economic, social and political activities easily. The conveyance of information in human life is superior to sometime before; and all developments on communication and IT is due to the presence and process of data (Sueb, 2013). In any case, this technological advancement might make a lot of dangers such as chance of data loss and system crash (Al-qattan et al., 2017).

In the contemporary networked world high availability of data is the key to existence of IT dependent organizations (Baham et al., 2017). The success and failure of an organization directly or indirectly depend on the availability and usage of data. And this data drives a worth of firm in multiple techniques; one it raises top-line income based on organizations investment on inventive novel products and service and second it upsurges profit of the lower line by systematizing resources management for internal supply chain through the Internet of Things (IoT) (Liu, 2017). Because of the IT activities are sensitive, all IT dependent companies are exposed to data loss. For fear of data loss, desire to be successful competent on the market and the issue of security aspect forces organizations to build their own data centers (Poskiparta, 2018).

Any act of damage to all and/or part of information technology infrastructures is IT disasters (Partio, 2017). Resources like staff, infrastructure, capital, and technology are required by business. However; most organizations focus only on the technological face and expect technology to be the core aspect for success. Though technology is certainly one of the core aspects for success, there are some occasions which can break the organization in seconds. That breaking occasion is disaster. A disaster, be it natural or human made, brings social, environmental and economic impacts (European Commission, 2020).

Telecommunications sector is vulnerable to different disasters, from those disasters Distributed Denial of Service is the main (Kaspersky Security Intelligence, 2018). Kaspersky adds the point that telecom sector was hit around twice as hard as the second placed sector (financial exchanges), with a median Distributed Denial of Service packet count of 4.61 million packets per second (compared to 2.4 Massively Parallel Processing for exchanges) by referring to the 2016 Data Breach Investigations Report. Immediate attacks can reduce network capacity, degrade performance, increase traffic exchange costs, disrupt service availability and even bring down Internet access if ISPs are affected. Kaspersky stated one example; during 2015 cyber-attack on the UK telecoms company, Talk Talk.

The hack, supposedly done by a couple of youngsters, brought about within the misfortune of around 1.2 million customers' e-mail addresses, names and phone numbers, as well as numerous thousands of client dates of birth and money related data. All ideal for utilize in financially-motivated social designing campaigns. Worldwide State of Data Security, 2016, IT security occurrences within the telecoms sector expanded 45% in 2015 compared to the year before. Telecoms suppliers have to be arm themselves against this developing disaster.

According to Global System for Mobile Communication Association (GSMA, 2019) telecom operators must give attention to their disaster recovery plans (DRP) so as to minimize threats such as Device Threats, Human Threats, The Internet of Things Threats, Cloud Threats, Signaling Service Threats , Supply Chain Threats and other threats. As (Rahman, 2017) said, the Global System for Mobile communication (GSM) works by inclusive acknowledgement of standards for cell communication. And this GSM passes through four territory assemble rules called Mobile Station, Base-Station Subsystem (BSS), Network and Switching Subsystem (NSS) and Operation Support System. So if there is any disruption in either of the territory the service will be unthinkable.

Telecom operators with their critical business elements are under fire from dual sides: one they face immediate attacks from cybercriminals damaging their organization and network operations, and two indirect attacks from those in search of their subscribers. Disasters comes from many levels: hardware, software and human (“Kaspersky

Security Intelligence," 2018). DR enables organizations to recover their data by continuously storing the data in internal and external servers. This DRP offers applications, servers, databases and storages that could assist the safety of the data (Sueb, 2013). After the occasion of September 11 75% of the IT experts began focusing towards DR (Bocian, 2009).

In order to assure their Business Continuity (BC) and get high customer satisfaction it is recommendable that telecom operators should work on data protection and service continuity by having an ITDR plan. Currently there are many different IT frameworks like Information Technology Infrastructure Library (ITIL), Control Objectives for Information Technology (COBIT), The Open Group Architecture Framework and Project Management Body of Knowledge (PMBOK).

However; those frameworks are very complicated and they took much more efforts for customization for companies to implement accordingly in addition to IT frameworks there are some ISO standards which explains BC and DR holistically. Further there are different ISO released standards like ISO 22301:2019 which describes about Security and resilience of BC management systems and ISO 27031:2011 which introduces a management systems approach to address ICT readiness for support of a broader BC management system (IRBCMS). Both follows the Plan=> Do=> Check=> Act (PDCA) management system which is holistically focused on BCM plan.

Based on the researcher's understanding level, the PDCA system does not clearly display the activities of ITDRP in the BC plan. And it is generic model for all organizations. Hence this thesis is aimed at developing an ITDRP framework for telecom sector specific to Ethiopian telecom provider (ethio telecom (ET)) which helps to fill the gaps in ITDRP for specific sectors in specific areas. And the will be developed framework solves the challenges on activities of ITDRP, for better data protection and uninterruptible IT services in the company. The study will give more insights to the management, experts and specialists in the company by giving right roadmaps on ITDRP preparedness and mitigation.

1.2. RESEARCH MOTIVATIONS

The motivation of this study are: 1. Researcher is interest to know why the company is quiet to provide permanent solutions to the occurring disasters in different time periods. 2. Researcher works there. The researcher has not simply involved to search on the already stated topic, but it is that the researcher had been part of the service interruption and data loss aching in the company. In behavioral research, examining inspiration is the consideration of human behavior.

Fundamentally why do individuals do what they do? The essential hypothesis comes down to two essential ways: Those are: - Internal components and external components. Internal components incorporate: being challenged by an issue and needing to actually discover a solution, finding positions or investigate in line with inner values and ethics, getting a work or finding fulfillment by doing something you need to do and willing to discover arrangements to major issues and offer assistance society. External components include: Looking for the endorsement of others, being respected for your supposition, requiring to realize a certain status and needing a great pay.

After researcher get an approval from the university research topic approval committee to conduct a research on the already stated area; another driving force come simultaneously with start of literature review: that driving force is there was no any provided work which discuses "A Framework of Information Technology Disaster Recovery" specific to the telecom sector and specific to Ethiopia. Further the researcher agrees with the motivations of previous studies done on the area of ITDRP. The motivations are presented under in a tabular form see below table.

MOTIVATIONS	FOUNDATIONS
The term disaster goes beyond the natural phenomena in Information Service Functions (ISF)	Wing Chow (2000)
Migration from centralized mainframe computers to distributed client/server systems has created a concern on data security	Steve M. Hawkins, David C. Yen and David C. Chou

Businesses continually increase their dependence on IT systems for routine business processes	Hossam Abdela Rahman Mohamed (2014)
Applications of ad-hoc DR standards and practices in organizations as there is no standard framework available	Mueen Uddin, Sandun Hapugoda & Roop Chand Hindu(2015)
Catastrophic natural disasters and malicious activities	Andrea Patricia Sanchez Dominguez (2016)
Manage responsibility of increasing resiliency	Bernard Koech (2016)
Manmade and natural disasters are threatening to interrupt core business activities	Mamdouh Alenezi (2016)
The need for continuity in IT operations even during a disaster	Dr.Khaled Shaalan (2017)
Explore the ITDRP current status in Ethiopian banks	Gerezgiher Haylay (2017)

Table 1: Motivation and needs for ITDR research compiled from scholarly works

1.3. STATEMENT OF THE PROBLEM

Ethio telecom; the monopoly telecom service provider in Ethiopia is currently providing all telecommunications services such as Global System for Mobile Communications (GSM), Code-Division Multiple Access (CDMA), Wideband Code Division Multiple Access, Long-Term Evolution (LTE), Fixed Line and all broadband internet service by owning many and different systems. Some examples of systems currently owned by ethio telecom are Customer Relationship Management (CRM), Internet Protocol Call Center (IPCC), Home Subscriber Server (HSS), Convergent Billing System (CBS) and others. However, the systems and data available in the company are unsafe from several potential disasters. Some obvious instances of the threats are power outages, hardware and software failure, human error, damage of communication link, virus attack, server air conditioning failures and sabotage.

As most of the systems are integrated each other a single link blockage or cut damages most of the systems of the company. As internal documents root cause analysis showed some of the practical disasters happened in the company are: 1. Call outage on April

2015 for three consecutive hours in the mid night. 2. SMS Service outage on February 2016-day time and complains were raised from customers specifically saying "we could not send message '**A'** to **8100**" higher managements were stressed and uniquely involved on pushing vendor experts and local experts to restore the service quickly. Unfortunately, it was not yet saved the 5 hours down time. 3. Call, SMS and internet services full stoppage on February 21st 2020 for consecutive 2:30 hours in the evening time. For this disaster Sheger FM radio 102.1 had asked "what the reason was" to the Chief Executive Officer (CEO) of ethio telecom; and the response of the CEO was "we faced a miner technical problem" shortly.

The 4th tragedy example in the company was internal email service outage and total email data loss on August 2018, May 2019 and February 2020. The problem happened on February 2020 was not only for email service outage and email data loss, rather it goes beyond to staff computers disaster due to virus infections. And it resulted to data encrypted by ransom ware to all of the infected computers in the company with different critical and none critical data. For the desktop computers formatting without restoring data was applied as a better solution. Email communication was stopped for 13 days without any solution; then finally total mail server formatting and changing new Active Directory was performed by the company as solution.

This sudden and repetitive service outages and loss of data remaining with no restoration; creates a big incite to the researcher's mind to study on ITDRF of the company. Many scholars have done their investigations and addressed different issues related to ITDR in different ways (see chapter two related works part). However, there was no work which addressed ITDRF for telecom sector. And the results collected from the preliminary study showed that ethio telecom has no ITDR in place rather it applies ad-hoc recovery techniques.

1.4. RESEARCH QUESTIONS

Based on the above detailed and brief discussions of the statement of problem and identified gaps, this study sets out to address answers of the following research questions:

1. What could ethio telecom be benefitted from attaining ITDR?

2. Why ethio telecom is challenged to have ITDR?
3. How ethio telecom can attain a feasible ITDR?
4. What are the possible criteria to select place to launch ITDR?

1.5. OBJECTIVE OF THE STUDY

1.5.1. GENERAL OBJECTIVE

The general objective of this study is to develop an ITDR framework for ethio-telecom.

1.5.2. SPECIFIC OBJECTIVES

The Specific objectives of this study are: -

1. To figure out the importance of having ITDR for telecom companies specific to ethio telecom.
2. To investigate the challenges to attain an ITDR in ethio telecom.
3. To study the current practice of ITDR and the means to have an ITDRF for ethio telecom.
4. To propose an ITDR framework.

1.6. SIGNIFICANCE OF THE STUDY

The investigations found that companies can minimize failure and loss of data from their mission critical and business critical systems by exercising ITDR. They can also improve data recovery and service continuity strategies via proper use of ITDRF. In general, this thesis has the significance:

- To give highlights related to the level of attentions towards ITDR in the company.
- To creates insights on company employees towards the use of data and ways of protecting it.
- To allow organizations eliminate definite risks or mitigate the impact of unavoidable disasters by reducing; disruptions of mission critical systems, likelihoods of occurrences and potential exposures.
- To expand understandings of IT experts and management in the company about the idea of IT disasters and their means of mitigations.
- To enable IT managers and firm leaders to keep business operations up 24/7 & avoid brand humiliation and ensure customer satisfactions.
- To create better awareness towards the advantage of ITDRF for the deployment of ITDR.

- To minimize expenses of initial investment due to lack of proper focus and operationalization for ITDR.

1.7. SCOPE (DELIMITATIONS) OF THE STUDY

The scope of this study involves investigations of current practices of ITDR in ethio telecom and moved up to developing a framework of ITDR for ethio telecom. The targeted areas of the organization to undertake this study was Addis Ababa at different divisions, departments and sections: Generally, this study covered the Information Systems Division (ISD) and Information Security Division (ISecD) and specifically higher managements (directors to managers), experts, supervisors, and specialists of the stated divisions. So, this study was not included other units due to the hugeness of the company.

To achieve the purpose and address the research problem specified previously, this research has performed a thorough analysis and review of the existing relevant ITDRF over the world. An assessment and crosschecking among previous works of the key elements for ITDR recognized in the literature review had accompanied by organizing them to formulate the conceptual framework which appropriate to ethio telecom mission critical and business critical systems.

1.8. ORGANIZATIONS OF THE STUDY

This thesis has five chapters, references and appendixes; which arranged as: - chapter 1 research introduction: presented background of the study area, introduced existing situations of the research topic, outlined context of the research. In chapter 2 literature review and framework development is presented and explained the significant and peer review literatures on ITDR with their effects.

Chapter 3 research methodology has offered highlights of the research approach and methods used to study the empirical learning. Also the Clarification of tool development for the study. Chapter 4 research analysis, result, revised framework and discussion: which discussed 1. Analysis and display the result of the research, 2. The construction of the modified ITDRF and 3. All new terms and definitions of ITDRF. In Chapter 5 conclusions, recommendations and future works are presented which offered

1. The effect of the study findings, 2. Limitations of the study and 3. Enumerations for future research tips. Finally, the references and appendixes are in closed to show sources of used materials in the entire thesis and the presence of thesis supplementary documents.

CHAPTER TWO

2. LITERATURE REVIEW AND FRAMEWORK DEVELOPMENT

2.1. CHAPTER INTRODUCTION

This chapter deals with literature review related to ITDR. It starts by presenting definitions of disaster, IT disaster (ITD), identifications of IT disasters, IT disaster recovery site (ITDRS), types of ITDRS and then goes in detail to ITDR, explanations, current state of the art regarding ITDR, types, importance, challenges and best practices of ITDR, related work containing (perspectives of scholars, focus, critiques and research gap), framework development, and then summarizes the chapter. Information Technology Disaster Recovery (ITDR) in service continuity and securing data perspective is still less explored specially in developing countries like Ethiopia as instance. Believing that literature review will give more light about the current status of the research in ITDRF and possible prospect research areas, an in-depth literature review has conducted. Accessible journal databases and top conference proceedings in information systems area were searched using different key words to gather significant resources for investigation.

2.2. DEFINITIONS AND TYPES OF DISASTERS

A disaster is an occasion or incident which brings considerable destruction in operational and/or computer processing capabilities for a period, which influences the operations of a business. Disasters can occur in many variety forms, and the duration can range from an hourly disruption to days or weeks of ongoing destruction (Gerezgiher, 2017). There are two kinds of disasters known as natural and man-made. Those both are separated in to fifteen classes crossing more than fifty subdivisions. Man-made disasters are classified into three other small classes. 1) Manufacturing accidents which includes involve physical infrastructure breakdown, bangs, ardors, gas outflows, injuring as well as radioactivity. (2) Transport accidents affected in earth both road and rail, flight, and water shipping services. (3) Mixt accidents: unexpected ardors and bursts, and failure of native and nonindustrial materials (Emergency Events Database (EM-DAT), 2019).

According to (Periasamy et al., 2016) disasters are investigated their causes; that some of them are dependent on affected place and some are due to knowing or unknowing human activities.

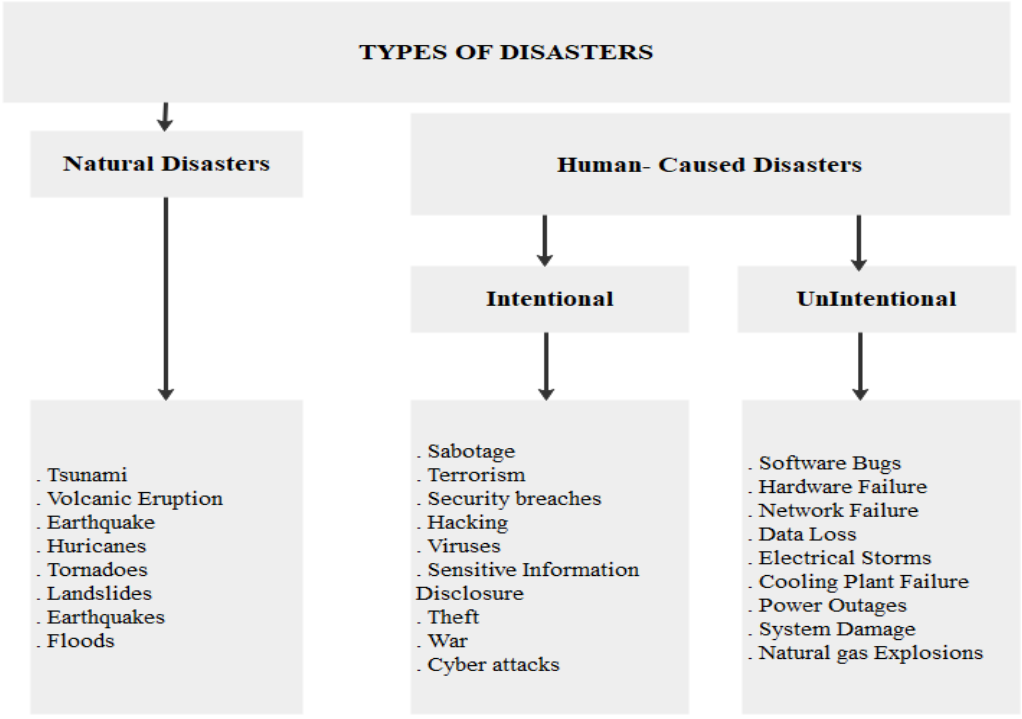

Figure 1: Types of Disasters collected from different literatures

2.3. IT DISASTER

IT disaster is all accidental service stoppages happened in small, medium and/or huge organizations resulted on not serving their customers. The outage may be hardware, software, data, information systems and networks. IT equipment related service route stoppages which they happened from data loss are possibly the most disturbing (Toigo, 2003). Toigo, in his book tried to show the dangerousness of disasters created from data loss comparing with other disaster. A Data loss disaster is the most problematic of all other infrastructures of a company or state to substitute. Data can loss by either unintentional or deliberate deletion of the data itself or obliteration of the data storage. (Toigo, 2003).

IT disaster is none warning happening resulted on destruction of IT infrastructures and causes vast losses in relation to the continuity of services and total existence of a firm (Alhaidari & Atta-Ur-Rahman, 2019). IT disaster is unplanned stoppage of IT services in a company; which includes critical and none critical systems service stoppage.

Example computer failure, corrupted data, lost data, network failure, software errors, computer virus, system abuse, hacking, human error to do operations, all ISP failure, power failure, system disconnection, damages to datacenter and other IT infrastructures due to human and natural phenomena (Rahman Mohamed, 2014). IT disasters varies from the unintentional removal of a file/folder to a storm which eliminates the firm which holds the data center and the surroundings (Shropshire & Kadlec, 2009).

2.4. IDENTIFICATION OF IT DISASTERS

Leonidas (2018), stated that there are many reasons of IT disasters; the common ones are: - Power Outages, Hardware Failure, Software Issues, User Error, Incorrect or Incomplete Training and Natural Disasters. According to a study by (DiDio, 2019) the following are the causes of IT disasters in technology firms. Those includes: - human error, security flows, bugs/flaws in server OS, IT dept. is understaffed/ overworked, server hardware too old/inadequate, instability of server hardware, server OS too old to run new computer, vendors too slow to issues patches, bring your own device, integration/interoperability, lack of documentation, configuration complexity, poor vendor technology support, lack of support for crucial applications, IT managers lack training, catastrophic events and mobility.

The most likely causes of IT disasters are fire, flooding, sabotage, theft, loss of facility support services, sustained power loss, sustained telecommunication failure and software malfunction (Spencer, n.d.). Disasters are not pre known and clear for any one, but depending on different damages happened to organizations, society, country and even the world disaster causes are rooted in to five. Those are development, governance, awareness and Perception, Political Environment and physical and Environmental Conditions (Witting, 2012). As (Uddin et al., 2015) said by referring to Bajgoric, the most significant reasons for IT disasters are software failures, planned administrative downtime, operator errors, hardware, outages/maintenance, building/site disasters (i.e. fire) and metropolitan disasters (i.e. storms, floods).

2.5. IT DISASTER RECOVERY SITE

“A DRS, also known as a backup site, is a place that a company can temporarily relocate to following a security breach or natural disaster. The site is just one facet of the

company's larger DR or BC plan (Smith, 2018)". ITDR Site can bring back data and keep an organization's IT system functioning during and/or after a disaster (Sembiring & Siregar, 2013). An area which organizations used to recuperate their IT services during or after a failure and unavailability of their primary datacenter is called DRS (Rouse, 2015).

An IT DR site is a DC which backup's data of a primary DC located physically far from the primary site of a company. The aim is to continue the functionality of systems at a time of disaster situations such as power outage, cyber-attack, network failure, natural disaster, unexpected downtime, sabotage or other occasion which makes unworkable to the main datacenter. The technology of ITDR site uses a remote access secured gateway from the primary datacenter and safeguards the operation of the company by supporting to minimize down time and Recovery Time Objectives (Robb, 2019). The below Figure illustrates how ITDR site uses a secured remote access gateway as a bridge between the primary and DR back up site.

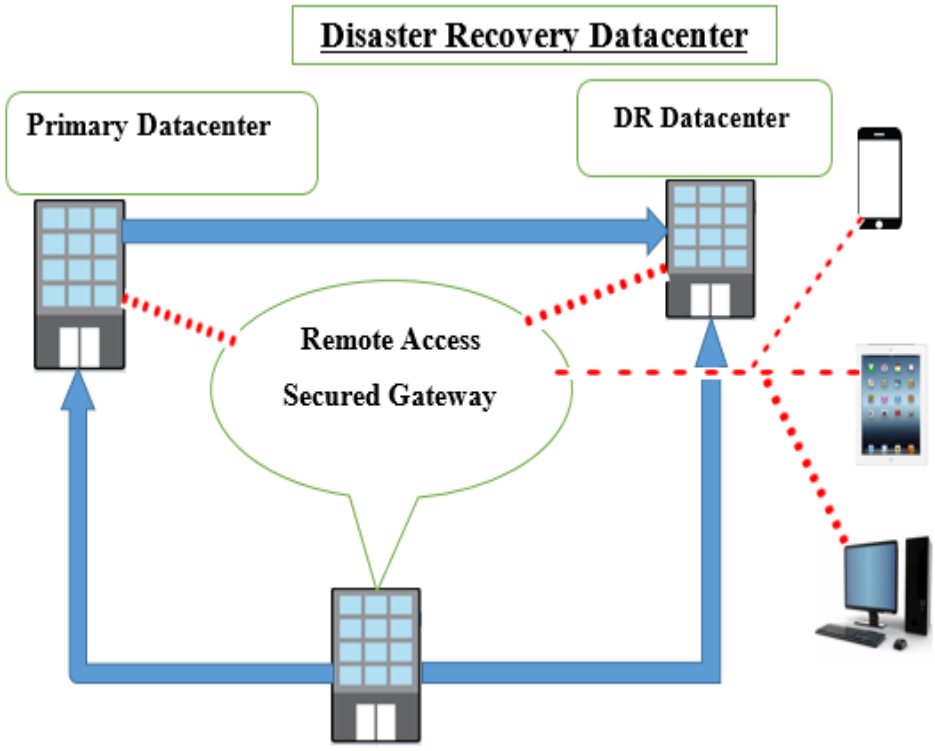

Figure 2: Illustrates ITDR site using a secured remote access gateway as a bridge between the primary site and DR site (Adapted from Robb, 2019)

2.6. TYPES OF ITDR SITES

There are two options of DR site known as internal and external. However, now a day there is also mobile site(Jessie Reed, 2019). By mobile site is to mean using a DR site in the form of trailers, and can be agreed in specific locations and fitted with the required technological infrastructure (Makwae, 2018). An internal recovery site is managed and lead by the company itself, whereas an external recovery site is arranged and managed by an outer third party provider. Internal recovery sites are frequently set up with complete access to the company's primary site data, which is best for a company that trusts heavily on its information. Though having internal site makes firms confident on, it is very costly to launch comparing with the external site. With those alternatives a company can apply one type of ITDR sites from the very common three types called hot site, warm site and cold site. And/or the other three uncommon one known as mobile site, mirrored site and wing site depending on its Recovery Point Objective (RPO) and Recovery Time Objective (RTO) (Jessie Reed, 2019; Robb, 2019; Shan Gupta & Changbin Gong, 2019).

Segue Technologies, 2013 states that the types of ITDR are three; hot site, cold site and warm site. According to (Uddin et al., 2015) there are four types of ITDR sites known as hot site, warm site, cold site and fault Tolerance Site. On the other side a book written by Evans Makwae (P. 32-34) has explained six types of alternate processing sites namely hot, cold, warm, mobile, mirrored and wing sites. There are two measures of objectives must fulfilled on the solutions compared to the cost expenses namely RPO and RTO (Marek, 2013; Omar Alhazmi & Yashwant Malaiya, 2012). RTO: The period in which business operating is inaccessible and must be returned. RTO is subjected to the activities desired to return the operation managing abilities at the backup server (Omar Alhazmi & Yashwant Malaiya, 2012).

RPO defines the extreme tolerable amount of data loss measured in time and the RTO defines the extreme tolerable amount of time needed to make functional to critical systems. Maximum tolerable amount of time for data integrity verification is determined by Work Recovery Time (WRT). The summation of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD). This MDT is used to explain the total amount of time that an organizational operation could be disrupted without

affecting any intolerable outcomes (Marek, 2013). Illustration of RPO, RTO, WRT and MTD is presented in the below figure.

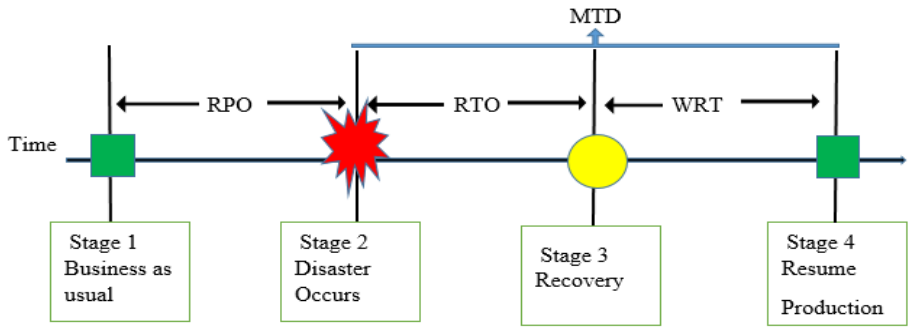

Figure 3: Shows the RPO, RTO, WRT and MTD (Adapted from Marek, 2013)

2.6.1. HOT SITE

Hot sites are basically mirrors of main DC. The backup site is settled with servers, cooling, power, and office space. The most important feature offered from a hot site is that the production environment(s) are running concurrently with the main datacenter. This syncing allows for minimal impact and stoppage to business activities. If there is some outage to the main DC, the hot site automatically starts working all the operations: This level of redundancy is costly and businesses should do the cost-benefit-analysis of hot site to use (Makwae, 2018; Segue Technologies, 2013). A hot site is a well-equipped back up site with having all the necessary IT infrastructures of the organization. A hot site is expected to be continuously connected and working without disturbance so as to ensure data synchronization between the sites (Hawkins et al., 2000; Makwae, 2018).

In hot site there is a necessity of employees and vendor support always for day and night operation. The tolerable RTO and RPO of hot site is 12 hours and 10 minutes respectively (Makwae, 2018; Uddin et al., 2015). It is a supplementary task of hot site to offer an exercisable strategy at the time of organizational recovery plan (Makwae, 2018). To implement hot site enough distance from the main DC should be a key requirement to control from affecting by same disaster to the DR and Production site (Hawkins et al., 2000; Makwae, 2018; Robb, 2019).

2.6.2. WARM SITE

In warm site every necessary infrastructure is ready, but not taking backups from the main data center. The difference among hot site and a warm site is that hot site delivers direct copy of primary site of a data center and its environment(s), but a warm site will make servers ready for the installation of a primary site (Hawkins et al., 2000; Jessie Reed, 2019; Makwae, 2018). Warm site fits to use non critical systems, but needs a level of redundancy. Warm sites contain all the elements of a cold site, adding to them additional elements such as storage hardware like tape or disk drives, servers and switches (Hawkins et al., 2000; Makwae, 2018).

Warm sites are operable after they get a copy of data. There is data harmonization done daily or weekly among the primary and the secondary sites with the consideration of small data loss. It is applied in companies having average level of error acceptance time. The operability of systems is one day with always ready for whole critical operational tasks in the site; there is no need of workers assigned. The RTO and RPO of warm site is 24 hours and 5-30 minutes (Uddin et al., 2015).

2.6.3. COLD SITE

It is just wired, air-conditioned and computer ready bare house (Makwae, 2018). A cold site is a built DR environment which functions by starting the tasks of restoring. Some IT resources are set but needs to initiate operating. As it is the cheapest one it is easy to launch for companies (Hawkins et al., 2000). A cold site has some infrastructures but are not connected each other, thus it needs important help from engineering and IT sections to get all essential servers migrated and functional (Segue Technologies, 2013; Shan Gupta & Changbin Gong, 2019).

In cold site there is a task of moving machines to the site, installation of operating systems and applications. This needs longer time, high coordination among company employees in different positions of security and computer vendor and others to deliver the machines to the site. All those operations takes too much down time (Makwae, 2018; Omar Alhazmi & Yashwant Malaiya, 2012). To implement cold site organizations must have high system stoppage tolerance with no need of assigning employees to the site. The RTO is 2 hours up to 3 days and RPO is 24 hours (Uddin et al., 2015).

2.6.4. MOBILE SITE

This recuperation location could be a self-contained flexible trailer that houses all of the computer devices. Most of these trailers are prepared with backup control generators, and can be prepared with all of the vital computer hardware as required. Though it may shift, the regular restoration time for a portable recuperation office is regularly a week or more (Hawkins et al., 2000; Makwae, 2018).

2.6.5. MIRRORED SITE

It is a completely an actual information processing site with equal and the same technical activities of the main site. There is high availability of data as data is concurrently processed in both sites. Such kind of sites are designed, constructed, run, and retained by the company (California Judicial, 2017; Makwae, 2018).

Mirrored site is equally furnished all necessary kits similar to hot sit. There are companies which they perform sending daily backup tapes to their mirrored locations so recovery will be done for current day's operation. Whether information are reflected or sent to the location, the startup time is ordinarily on the same day (Hawkins et al., 2000; Makwae, 2018).

2.6.6. WINGING SITE

In such type of choice there is no alternative site located somewhere or a backup plan for the organization. Hence companies performing identical to this technique regularly fail more than they succeed in rearranging their computer systems (Hawkins et al., 2000; Makwae, 2018).

2.7. IT DISASTER RECOVERY PLAN

ITDRP is a document which includes policies, processes, procedures, rules and regulations so as to provide feedback during and after a strike. DRP is the aim of restoring information systems at a time of catastrophe to the commercial datacenter of a company which basically focused on data and application. It is a type of organizational activity for BC by giving attention to avoid business interruption and keep on healthy functionality for mission-critical business functions (Periasamy et al., 2016).

DRP is type of organizational activity for BC, because DRP is a core component of BC. BC has four core components which are Business Impact Analysis (BIA), DRP, Crisis Management (CM) and Work Area Recovery Plan (WARP) (Telecom Excellence Academy, 2017).

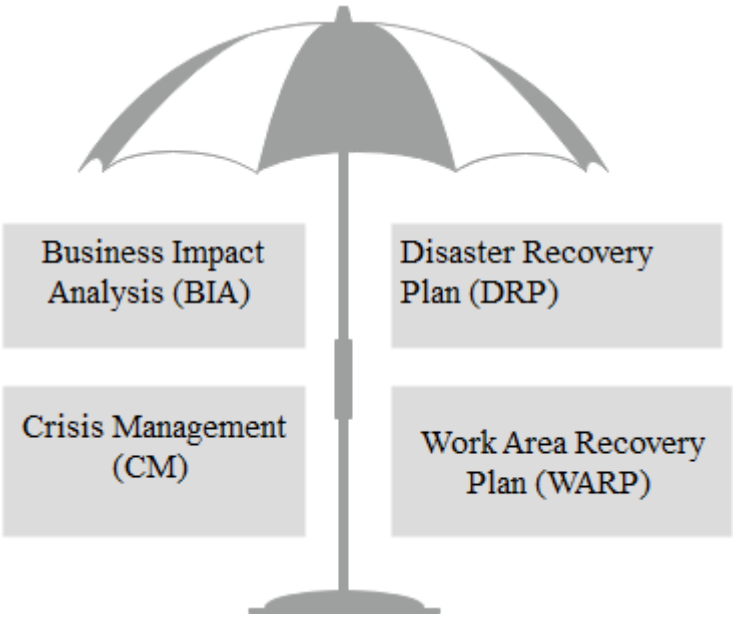

Figure 4: Core components of business continuity (Adapted from Telecom Excellence Academy, 2017)

ITDRP is defined as continual task of planning, developing, testing and applying of ITDR administration steps and procedures. This is done to confirm the effective and actual continuation of important commercial activities in the occasion of an unprepared pause. ITDR is part of BC, and deals with the immediate impact of an event on IT infrastructures (Rahman Mohamed, 2014). As (Somasekaram, 2017) explains DRP has many components and its class is under IT related recovery tasks beginning form IT inventory and IT risk analysis.

Recovering from a server outage, security breach, or hurricane all fall into DR category. DR usually has several discreet steps in the planning stages, though those steps blur quickly during implementation because the situation during a crisis is almost never exactly to plan. DR involves stopping the effects of the disaster as quickly as possible and addressing the immediate aftermath. This might include shutting down systems that have been breached, evaluating which systems are impacted by a flood or earthquake, and determining the best way to proceed. DRP is a collection of Business Continuity

Plan responsible for a direct influence of an occurrence. Therefore, companies need to address the potential disasters that will challenge their ability to stay with in an operable business and generating income (Snedaker, 2013). BCP and IT Disaster Recovery Planning (ITDRP) are the focal incident management plans that are realized by organizations in order to safeguard any business interruption and reply to whichever disaster occurs (Wunnava, 2011).

An ITDRP is a documented procedure or set of processes to recuperate and safeguard an IT infrastructure in the occasion of a disaster. The DRP, normally documented in written form, states procedures that an organization should follow in the event of a disaster. It is a full statement of reliable activities to be taken before, during and after a disaster. The disaster could be natural, environmental or man-made. Man-made disasters could be deliberate or accidental (Stouffer et al., 2015).

According to (Stouffer et al., 2015) the DRP is vital to sustained availability of the Industrial Control Systems (ICS) and should include the following items.

1. Required response to events or conditions.
2. Procedures for operating the ICS in manual mode.
3. Roles and responsibilities of responders.
4. Processes and procedures for the backup and secure storage of information.
5. Complete and up-to-date logical network diagram.
6. Personnel list for authorized physical and cyber access to the ICS.
7. Communication procedure and list of personnel to contact in the case of an emergency.
8. Current configuration information for all components and
9. Schedule for exercising the DRP.

The plan should also indicate requirements for the timely replacement of components in the case of an emergency by having guiding policy. The policy includes important points such as speed at which data or the system must be restored, the frequency at which critical data and configurations are changing, safe installation media storages license keys, and configuration information, safe onsite and offsite backup storage and identification of individuals responsible for performing, testing, storing, and restoring backups.

ITDRP is a plan designed to recover all the important business processes during a disaster with in a restricted amount of time. This plan has all the ways required to handle the emergency situations. A DR process should have demonstrable recovery capability, and hence it provides the most efficient method to be adopted immediately after a disaster occurs. Mostly the DRP has technology oriented methodologies and concentrates on getting the systems up as soon as possible, within a reasonable amount of time (RTO and RPO). RTO and RPO are the recovery time objective and recovery point objective, which are the targets of DRP. “The most successful DR strategy is the one that will never be implemented”; therefore, risk elimination is a serious component in the DR procedure (Jorrigala, 2018).

As presented by (Shan Gupta & Changbin Gong, 2019) about RTO and RPO: - RTO is the target time that is necessary to return all applications smooth activities after the occurrence of disaster. The main target is to measuring the speed of service restoration from disaster. It is usually known that very important applications must have lesser RTO.

The RPO is the considerably acceptable amount of lost data within that time frame or it is the measurement of the applications ability to tolerate for how much data loss fairly to accept with in that time. RPO is about how much data an organizations application can afford to lose in a disaster situation. To build an ITDR plan that secures the survival of applications after a catastrophe and is also cost effective, companies must consider both RTO and RPO. At the same time organizations should confirm that both RTO and RPO goals can be realized to recuperate healthiness of applications successfully from a catastrophe.

DRP is a document with full detail discussion of different steps to build and operate recovery tasks, such as forming DRP team and steering committee, performing risk analysis and BIA, developing recovery strategies, implementing testing and training tasks, auditing and reviewing the plan (Periasamy et al., 2016).

2.7.1. ELEMENTS OF IT DISASTER RECOVERY PLAN

According to (Snedaker, 2007) for the aim of ITDR there are three useful components named people, process, and technology. As technology is the required element

performed by people following different processes; the process element by itself is a technic of alignments of tasks to achieve the specific need. However, technology is merely perfect if the people who did it are genius and have done the technology by fully understanding its objectives. According to (Accelerite, 2014) the focus of companies should be targeted on the fit of three chained components (People, Processes and Technologies) so as to become better prepared for disasters.

People: - are the experts or actors of tasks in the real ITDRP and performers of it. Even though ITDRP is fundamentally about the IT activities, the people involved in the DR planning would not limited to IT department it must be inclusive from other departments and managements.

Process: - is a document having all the tasks and operations to be performed by the actors.

Technology and Infrastructure: - are equipment's used by the actors at the time of disaster so as to restore the operation to its normal scenario. Rarely infrastructure is separately discussed from technology to magnify its importance, but it is actually part of technology. The below Figure illustrates elements of ITDRP.

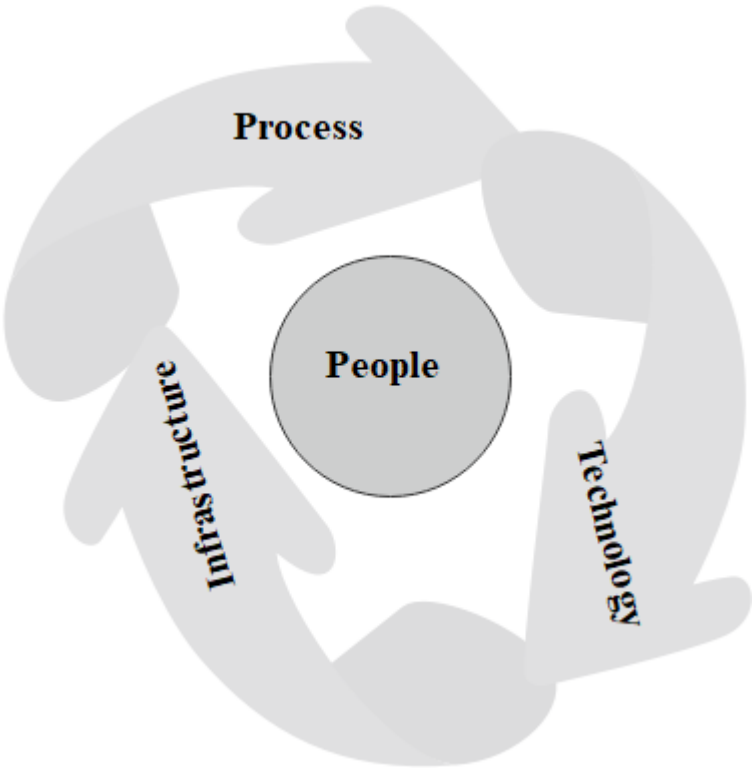

Figure 5: Interactions of BC/DR elements (reprinted from Snedaker, 2007 p.6)

2.7.2. STRATEGIES OF ITDRP

DR strategy is intended to certify that the persistence of vigorous business routes in the occasions that a catastrophe happens. It offers an operative resolution that can be used to recuperate all vigorous business routes within the essential time frame using vigorous archives that are warehoused off-site (Martin, 2002). The last step involves designing the conditions for the plan test and maintenance. Planning without testing can be catastrophic. A disaster recovery plan must wisely test and tweaked as necessary.

The most important thing in DR strategy is testing strategies of the DR. This includes plan, introduction, test teams, pre-test planning, test timeline, critical test and test problem log (Adedayo, 2014). An organization may develop new products needing new or better routes. It is obligatory to contain the outcome of these changes into its DR plan to make sure that it is up-to-date and ready to implement when the next business interruption occurs (DR Test and Maintenance, 2010).

The recovery strategy is aimed to relocate critical Information Systems processing to an alternate computer-processing center. The processes will be recuperated at the DR provider name and location of the Site. The DR services provider name is responsible for ensuring that the system configurations and the related network desires are exact and technically viable at all times. Therefore, yearly testing will be a part of the alternate processing strategy. Also, the associated network connectivity will be recovered, within the disaster recovery scenario, using the alternate processing strategy (Makwae, 2018).

2.7.3. PHASES OF IT DISASTER RECOVERY PLAN DEVELOPMEN

Previous literatures have raised different ideas in their work with regard to diverse planning phases applied in developing DRP. To develop an ITDRP a number of steps are required; however those steps are not equal by the view of researchers and are presented in different ways (Joe, 2013). According to (Sedaker, 2007) Contingency Planning Policy, Risk Assessment (RA), BIA, develop BC and Recovery Strategies, develop DRP, awareness testing, and training and maintenance and exercise are the seven phases in an ITDRP development. As mentioned by (Iyer & Mastorakis, 2006) IT DR cycle has four stages namely risk reduction/ Prevention, readiness, response and recovery. An ITDRP process passes through five very essential phases known as Project Initiation, BIA, Developing a DR Plan, Testing a DR Plan and Maintaining a DR Plan

(Luckey, 2009; Mark Flesch, 2019; Mark Pelt & Tom Baker, 2017; Pritchard, 2019). Those phases are discussed below.

1. Project Initiation: - It is the basic to fix and create main objectives and fundamental elements of the project. Actual project initiation process easily supports to the achievement of the ITDRP (Luckey, 2009; Mark Pelt & Tom Baker, 2017). The main tasks of this phase are Project arrangement, securing management support, organizing the planning project team, establishing the project management process, obtaining the required resources and developing initial project objectives.

2. **BIA: -** In this stage tasks are all about knowing criticality of operations so as to keep the operation always functional and considering the influence of the interruption of these process on the whole business. It gives an emphasis to the core departments with holding critical system and data access (Luckey, 2009; Mark Flesch, 2019; Mark Pelt & Tom Baker, 2017). Tasks such as gathering information, identifying the time-critical IT systems, performing a RA and prioritizing the recovery efforts are included.

3. **Developing ITDR Plan: -** Depending up on the analyzed information at BIA phase, in this phase specific processes and procedures should be identified and documented for the usage at a time of disaster. Activities like selecting the risk management strategies, defining disaster severity levels, Identifying activation triggers, defining and documenting specific recovery processes and selecting disaster response team members are the main to be performed (Luckey, 2009; Mark Pelt & Tom Baker, 2017; Pritchard, 2019).

4. **Testing ITDR Plan: -** Once the plan has been established/ developed, it is a must to be tested and audited to confirm either or not it could achieve recovery objectives. Key activities includes developing test strategy, training the recovery staff, conducting test procedures and establishing test frequency (Luckey, 2009; Mark Flesch, 2019; Mark Pelt & Tom Baker, 2017; Pritchard, 2019).

5. **Maintaining ITDR Plan: -** It is an obvious that there is continuous change and transformation in an IT industry. So the ITDR needs none stopping provision and maintenance to be fit to the existing system/ business necessities. The mandatory tasks

are identifying likely sources of changes, selecting change management strategy and maintaining the planning documentation (Luckey, 2009; Mark Flesch, 2019; Mark Pelt & Tom Baker, 2017; Pritchard, 2019).

2.7.4. ITDRP TESTING TECHNIQUES

After developing the ITDRP testing is mandatory to evaluate its functionality and fitness with business need. BIA done in the development stage supports to know critical business systems. And testing is important to certify the familiarity of staff with the operation. Testing requirement should be done periodically depending to the organization need. But if there is some system updates testing the ITDR must be performed finishing that update to the mail site (ITmanagers, 2013). All sensitive systems stated in the plan should absolutely tested based on the test procedures. Testing in an iterative way which is recommendable to organizations, brings none stopping ITDRP development (Krocker, 2020).

A company may have abundant reasons to test the ITDRP but the first one is to cross check fitness of the plan with regard to business requirements. And then approve its functionality at a time of actual disaster. Then the other reasons may be to check processes, procedures, and steps; to authorize the incorporation of activities within different business elements and management functions; to assure either the right equipment's have been set properly; to introduce all concerned bodies with the complete process and movement of information; to investigate gaps or weaknesses in the plan and to control cost and feasibility (Snedaker, 2007). There are different approaches of testing ITDRP, but the mostly used approaches are table top, walk through, isolated simulation, integrated simulation, full simulation, parallel testing and full interruption testing (Flinder University ITmanagers, 2013; Krocker, 2020; Sedaker, 2007).

Table top: - It is performed by both owner and other users along with reading details of documents for evaluation of correctness and put that hypothetically important to give real recovery procedures.

Walk through: - is a task of oral walk through the stated procedures in the document including evaluation about weakness and strength of the plan. To perform such test there must be previously confirmed list plan tests. It is useful to provide the chance of

participating huge members of team and make all informed about actions to be done, offsite systems to be restart and shutdown and infrastructures to be included.

Isolated simulation: - a test which includes live activation of the testers with real and theoretical cases to be tested to specific application of infrastructures.

Integrated simulation: - An action
of realistic and theoretical activations of plan to test multiple applications and related infrastructures to show the ability of restoring every critical system.

Full simulation: - This testing is performed using live activation of the team through above one level of the organization by real and theoretical scenario to every critical system. This kind of testing is very strong testing and it is realistic.

Parallel testing: - is testing with checklists and/or simulation tests. Previous business transactional data are administered against the last days of back up files at the DR site.

Full interruption testing-this test activates the whole ITDRP, but this test disturbs the usual process and operations for that it must be applied with high carefulness. To validate the ITDRP according to the business need checklists have huge role.

2.7.5. IMPORTANCE OF IT DISASTER RECOVERY PLAN

The holistic advantage of DR is it maintains BC. A website of COMPUVAULT secure data protection has posted the summarized research result of University of Minnesota and University of Texas against Catastrophic data loss as follows. The University of Minnesota found that “93% of businesses that misfortune their information center for 10 days or more recorded for liquidation inside one year.”

The University of Texas ponder says "companies that endured a disastrous information misfortune, 43% never revived, as it were 6% survived.” Those two universities findings show how important is working on DR for companies’ BC. Creating an ITDRP helps to distinguish different steps in an organization to recouping from data losses and reestablishing information resources. Securing the implementation of ITDRP helps to minimize the cost of loss at a time of disaster (Makwae, 2018). A company with unsatisfied customers is not competitor of other similar service providers, so having an ITDRP leads to good customer satisfaction as it merely supports the business to run without interruption. If an organization is serving its customer with highest satisfaction it really creates peace of mind (Gustafsson, 2018).

A company with worthy ITDRP can get benefits like long-term gaining revenue, increased productivity, avoids replacement costs and keeps good reputation (Brooks, 2019). Communications infrastructures are serious to an effective DR process to alleviate the opposing influence on life and property. However, communications infrastructure is among the major to get severely injured in disasters. At that time making communication becomes very difficult or totally impossible. Applying ITDRP safeguards organization's IT asset and able to run their IT operations efficiently. It is important to have ITDRP to protect data loss occurred from human error, unexpected updates, fire and power outage (Admin of Open Minds, 2018).

According to (Evolve IP, 2018) there are four basic significances of ITDRP. Those are Cost-Efficiency, increases employee productivity, very good customer retention and better understanding of scalability. Developing ITDRP helps to companies in restoring data from loss and keep all IT facilities on providing required IT services (Ghannam, 2017). According to Hawkins et al., (2000); and Makwae, (2018) having ITDRP has seven core importance. Those advantages are: -

1. It eliminates confusion and human error: - It is meant that at the time of any disruption specific assignments are given to responsible assigned team and other administrative groups will give their attentions to other important tasks required to the recovery activities.

2. It reduces disruptions of corporate operations: - If there is pre-established ITDRP with assigned team, at the time of any disaster there will not be chances to consume time to do new staff assignment.

3. ITDRP offers alternative options for mangers to consider: - The DRP gives variety of options at the time of no disaster to management members to think about what they should do if disaster happens.

4. **It reduces dependence on certain key individuals: -** If for example there is a destruction of voice and SMS services separately; on a telecom company and there are two or below two staffs who are experts on that area and are not present at the time of the event this staff dependency creates additional problem.

5. **It protects the data of the organization, which is the most invaluable asset of an organization: - Data** is the priceless resource of an organization; and if a company has ITDRP it stores its data securely depending on its sensitivity.

6. **It guarantees the security of company employees: -** A DRP could also include a logistical support group that would provide comprehensive support to employees.

7.. It efficiently supports for sequential and smooth recovery: - Serious events are requiring short and sequential recovery.

2.7.6. BEST PRACTICES OF ITDRP SERVICES

To have a one type of ITDRP implementing mechanism over the glob is very difficult as IT companies have different IT infrastructure and type of services to be addressed to their clients. However, there are commonly shareable practices which includes: analyzing IT Services, Preparing Organizational members, devising means of IT disaster identification and notification, developing procedures for restarting IT services and systems, creating a schedule for backup procedures, selecting offsite storage facilities, creating maintenance schedules (Kadlec & Shropshire, 2010). To organize effective ITDRP, identification of the risks, putting explanations, listing the procedures, performing review of backup plans, doing innovative tasks on ITDRP and accomplishing necessary preparations are key tasks to be performed (Calik et al., 2013).

According to (Cisco, 2008) the primary step in arranging recuperation from unpredicted catastrophes is to distinguish the dangers or dangers that can bring around catastrophes by doing hazard investigation covering dangers to business stability. A book written by Makwae p.31 discusses that the intial point for DR implemtation as best expirences is that developing strategies for DRP which includes: - Doing RA, recognizing imaginable vulnerabilities (weaknesses), preparing a plan of action, selecting an alternate recovery site, choosing a backup mechanism, performing a verbal walk-through and examining the plan on a regular basis to ensure its reliability. ITDRP best practice is the applied working experiences of an IT functions for all the catastrophe recuperation exercises depending on ITDRP components. The ITDRP components incorporates; IT catastrophe distinguishing and Notice, IT administrations investigation, arrangement of the group and plan improvement; and creating plan for reestablishing IT services (Hassan, 2017). Best practices and strategies are built up to form values and minimize hazard. It is accomplished through usage of IT control frameworks. A framework could be a frank or conceptual structure that guides development of a structure into a more valuable shape. Framework as holistic speech are two types called theoretical or conceptual (Dickson Adom et al., 2018).

RA is raised by different scholars as best practice to develop ITDRP. The researcher tries to discuss what RA is and the types of risks as follows as a continual of best practice for ITDRP implementation. As (Munteanu et al., 2008) defined RA by referring to (Karim, 2006:190-191) it is the "process involving assessing threats, vulnerabilities, and risk, evaluating and selecting security measures to reduce identified risk and implementing and monitoring the selected measures to assure that the measures are effective. Risk management is truly a management process." RA is a procedurally task of characterize the system, identify threats, identify vulnerabilities, analyze risk, identify recommendations and document results respectively (Leidinger, 2004).

(Cisco, 2008) describes that RA is a process of extracting list of vital functions of an organization's systems and measuring them with regard to the likely hood threats and vulnerabilities. Tasks of assessments to threat, vulnerability, impact and risk are the common activities. Those main activities of investigations are used for all five types of risks called external risks, facility risks, data systems risks, departmental risks and desk-level risks. Implementing different IT frameworks and performing valuable customizations so as to implement different IT services is a best practice of IT dependent organizations. It is recommendable for developing improved ITDRP (Chowdhuri, 2011).

In IT a framework is a platform which supports and guides IT companies to perform activities based on selected and agreed frame or model. The agreed model or frame is a mirror of how systems are interdependent each other (TechTerms, 2020). Some very important experiences of ITDRP stated by (Jines, 2018) includes: have a written plan, Keep a copy of data off site, test your plan with realistic scenarios, make updating the ITDRP part of change management process and plan for resuming normal operations, too.

Accomplishing RA in an organization supports to decide the type of ITDR model should to be own. After the attack of United States (US) by terrorist groups on September 11, 2001 (9/11), many companies are giving good emphasis to risk management in order to secure their assets by performing RA, emergency management, BCP, DRP and crisis management (Zhang & McMurray, 2012). According to AT&T

corporation for any business to have excellent continuity the following are best practices of ITDRP: Identify key business processes and impacts; perform RA, risk treatment and management; determine recovery strategies; develop BC/DR plans (train, test and exercise the plan and monitor and improve performance).

2.7.7. CHALLENGES INFLUENCING ITDRP IMPLEMENTATION

It is always true that successfulness in fiasco (disaster) management rely on /fiasco plans that has been done formerly by harmonizing whole units of an organization on providing specified trainings for IT disaster related tasks (Calik et al., 2013). Absence of administrative involvement, IT involvement, human resources services such as (training and promotion) can influence ITDR executions. According to (Chow & Ha, 2009) if organization's are not aware of 14 factors of successful ITDRP namely: (Top management commitment, Policy and goals, Steering committee, RA and impact analysis, Prioritization, Minimum processing requirement, Alternative site, Backup storage, Recovery team, Testing, Training, Documentation, Maintenance and Personnel participation), it is totally a dream to develop ITDRP.

(Chow, 2000), organizations should work seriously on 17 critical success factors to avoid negative influence and challenges of developing their ITDR. Those factors are known as:- Top management commitment, Adequate financial support, Alignment of DRP objectives with company's goals, Adoption of project management techniques, Presence of a formal recovery planning committee, Participation of representatives from each department, Engagement of external consultant, RA and impact analysis, Determination of maximum allowable IS downtime, Prioritization of IS applications, Off-site storage of backup, Presence of emergency response procedures, Training of recovery personnel, Appropriate backup site, Periodical testing of DRP, Maintenance of DRP and Insurance coverage for IS loss. The ITDRP difficulties are studied because of four challenges or factors termed as technology, organization, environment and individual (Hoong & Marthandan, 2011).

Even though there are many challenges influencing success of developing ITDRP, the main challenges are that organizations lack or have poorly implement the following nine important activities (Ghannam, 2017).

1. **Top management support**: ITDRP is a long-term process that requires a significant investment by an organization. Therefore, this plan requires top management support to secure resource and money for developing, testing and maintaining the ITDRP plan. Management should be responsible for coordinating the activities of DR plan and confirming the effectiveness regarding this plan within the organization. Moreover, management has to acquire the resources like time and budget in order to develop an effective plan.

2. Sufficient financial support: the big challenge associated with initializing effective ITDRP is the total cost for developing, testing and maintaining the plan. This cost is considered too high besides that the ITDRP has no immediate return on investment. Therefore, sufficient financial support is crucial to achieve successful ITDRP.

3. Alignment of ITDRP objectives with business goals: the business aims of an organization have to align with ITDRP objectives. These objectives of ITDRP define and set during the initial phase of ITDRP, and these objects can be considered as a guide for ITDRP.

4. Off-site Backup: off-site storage backup is a critical part during applying ITDRP, it provides organizations to restore their information in case of disaster. Off-site backup involves backup hardware, software, and data files. Location of the off-site storage should place in an area far enough from the organization.

5. Choosing an alternative site: create an alternative site to replace the original site is vital of having an effective ITDRP. The alternative site considers an optimal solution to respond to the natural disaster like earthquake or flood which can destroy the original site. There are multiple options to be considered when building the alternative site such hot, warm and cold site. All these options are possible to choose based on the budget and the acceptable length of downtime.

6. Maintenance and update of ITDRP: efficient ITDRP have to be updated and maintained. Therefore, ITDRP must reflect the new changes in business strategy and the changes in information systems including hardware and software. The importance of maintenance ITDRP is to reduce wrong decisions, decrease the stress of DR team during the recovery process and to keep the plan updated with changes in information technology and business operations. Once ITDRP plan is developed, there is need to monitor changes in the organization which have a significant impact on ITDRP. The changes in IT infrastructure, systems and the business operations have the biggest impact on IT DRP. Beside the changes in IT infrastructure and business operations

which requires to update ITDRP. Changes in operations, legal and regulatory have to be monitored and considered in ITDRP.

7. Continuous testing of ITDRP: ITDRP should be tested periodically in order to make sure that ITDRP complete and valid. Recovery team members have to perform simulation exercises. These exercises include training to handle all kinds of disasters. Conducting such exercises will make ITDRP more accurate. The test of ITDRP is vital to train team members on how to use this plan on their duties and roles and how to communicate across the organization. Moreover, testing this plan will help to correct the wrong steps, procedures and checklist.

8. Adequate trained Staffs: having a staff with proper training is vital to have an effective ITDRP to solve problems in case of disaster occurs. Staff members have to understand their duties and responsibilities to ensure accurate and fast deploying of ITDRP procedures. Developing a clear and measurable outcome from the training is essential to have more effective training. This includes the basic requirements for the training and the expected learning outcomes. Moreover, he mentioned that the training on ITDRP should involve training staff members on the specific roles and activities during implementing ITDRP. Training is essential to ensure that all staff members understand their roles, to reduce the potential operational errors and the chance for the miss communication when the plan is implemented. Many companies have a limited time or funds available for training. The training on ITDRP and is considered more difficult compared to the normal training.

9. Perform RA and BIA: RA and BIA have to conduct in order to have cost-effective ITDRP. RA address all possible threats to IT services and information systems. BIA determines the impact of the business processes if it became out of service and determines the maximum allowable downtime.

2.8. RELATED WORKS

Previous works reviewed with regard to the topic, problem statement, research question and objective of this thesis are termed as related works. To get exactly fit previous works the researcher performed different searching mechanisms without limiting published time. Unfortunately, no exactly relevant previous work has found in telecom sector locally in Ethiopia or internationally elsewhere. However, some very relevant attempts were found exploring same issue in banks and slightly attempts in smart city,

state counties and IT companies. The first relevant work was done in bank and has tried to develop an ITDRF for Sri Lanka Commercial Banks (CBs), second relevant work tries to develop ITDRPF for service continuity in smart city of Abu Dhabi Smart Government. Third pertinent literature tries to develop evaluative framework for IT Service Continuity (ITSC)/DRP in Kenya's counties. The fourth and fifth works were done in Ethiopian banks related to current status and practice assessment. The sixth considered relevant work has addressed a component based BC and DR for IT companies. So the researcher decided to see what has been done by them irrespective of the industry difference.

The paper by (Uddin et al., 2015) was aimed to develop DRF for Sri Lanka CBs and the authors have assessed the ITDR practices. Based on their investigation the most significant reasons for system downtime are 1. Software defects/failures 2. Planned administrative downtime 3. Operator errors 4. Hardware outages/maintenance 5. Building/site disasters (i.e. fire) 6. Metropolitan disasters (i.e. storms, floods).

In their work they include different international standards which helps developing new ITDRF for CB of Sri Lanka like BS25999-1:2006, BS25999-2:2007, ISO/IEC 24762:2008, BS 25777:2008, ISO 27001 and ISO 27002. In their analysis result report the researchers put that even though most of the banks in Sri Lanka have adopted ITDR approaches that supported by the regulatory guidelines of the central bank, the practicality of the plan is still uncertain. Finally, the researchers recognized that the current ITDR in Sri Lanka CBs are not realistic as well as not maintained by internationally accepted standards. For that reason, they proposed new ITDRF which supports top level manager to develop step-by step approach realizing ITDR exercises in their particular banks. The proposed framework looks like the below figure.

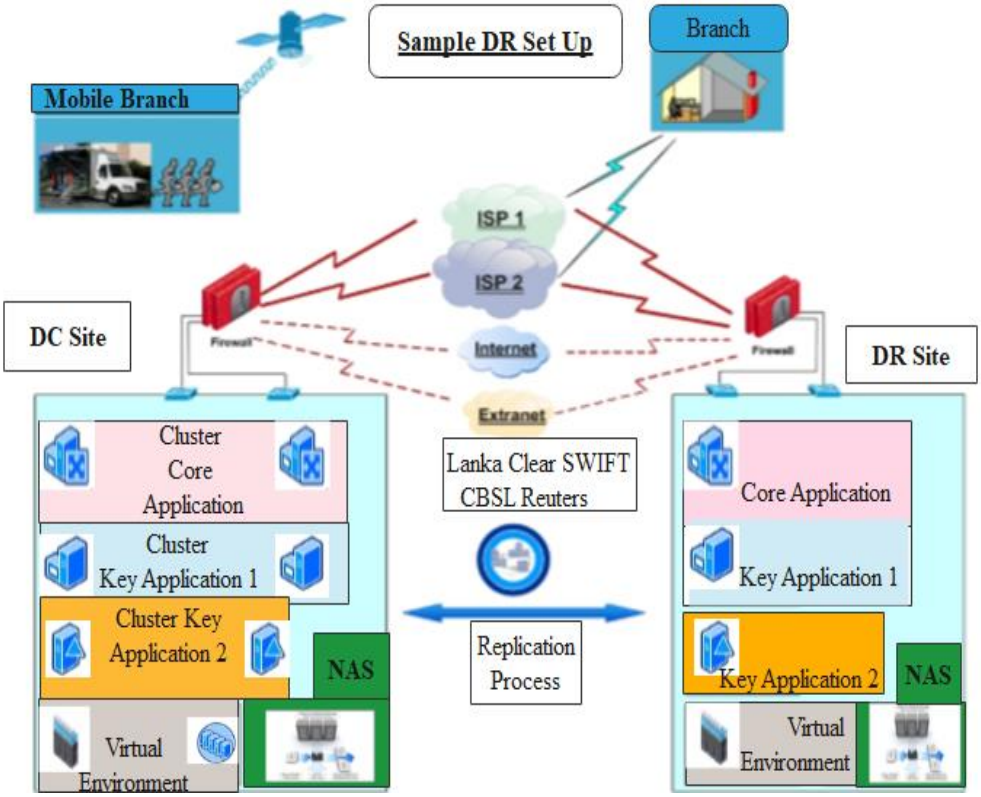

Figure 6: Sample ITDRF set up (Reprinted from Uddin et al., 2015 P. 277)

The proposed framework was tested by 12 domain area experts including representatives from the central bank of Sri Lanka in a standard questionnaire format. All questions were scaled from 1 to 5, where 1 represents the areas that need improvement and 5 represents excellent work. The proposed framework According to the results, the methodology, analysis, and artifact were accepted and the framework was considered adoptable by the CBs in Sri Lanka (Uddin et al., 2015).

A thesis presented by Hassan (2017) entitled "Information Technology Disaster Recovery Plan (ITDRP) Framework – A study on IT Continuity for Smart City in Abu Dhabi Smart Government" had aimed at developing ITDRF for ITSC in Smart City specific to Abu Dhabi. She tried to assess and investigate the ITDRP practice in smart cities; based on her investigation there were three factors (people, process and technology) influencing smart city services and six components (implementation, continuity, people, technology, organizational and environment). Then depending up on the factors she identified in the literature review that means factors influencing smart city services and the components of ITDR, she has developed a conceptual framework.

She reread different international standards including ITIL, IT Service Management (ITSM), COSO and COBIT for the purpose of getting support in developing ITDRPF. She has applied a qualitative research method as a research design. Her sample was experts, IT professionals and policy makers of Abu Dhabi Government and United Arab Emirates. She has performed detailed statistical analysis to identify the relationships between the key variables i.e. smart city services and ITDRP and the way of framework implementation at a time of IT disaster.

Finally, she has identified the factors influencing smart government services in smart city were (Technology (IT and Skills), Processes, People, Organizational (Culture/ Structure), Financial Resources, and Security & Privacy. And the core components of ITDRP were (implementation, continuity, people, technology, organizational and environment). Then she conjoined them together and formulate a revised framework. In here finding she has listed Smart City Components were: People, Process and Places, ITDRP Components were: Financial Resources, IT Implementation, IT Continuity and other components were: experience and education.

A research presented by Koech (2016) entitled "Evaluation framework for ITSC and DRPs: the case in Kenya's county governments" was aimed to assess implementation of ITSC initiatives in Kenya 's County governments and to develop an evaluation framework to evaluate ITSC and DR programs on Information systems in Kenya 's counties. He reviewed different literatures to come up with the final evaluative framework including internationally accepted IT frameworks like ITIL, Projects IN Controlled Environments (PRINCE2), COBIT, ISO27000 and Committee of Sponsoring Organization.

In his review he has written the nature existing IT Service Management and IT Governance frameworks listed above are prescriptive and do not show how to implement. They rather only show what the IT function must have and this makes them difficult and complex to know as even they don't have direction for how to implement. In addition to this in his investigation the existing frameworks are expensive and weighty to apply them in small to medium organization for ITSC system evaluation. He added that currently business and organizations rely more on systems than ever before. He realized that there is no sole methodology that can ensure 100% full recovery

after a business distraction. But if companies adopt different standards with possible customizations for best criteria of ITSC, they may become profitable. He assures that an effective ITSC planning framework assures information availability and its survivability. He has explored that there is, low implementation of ITSC/DRP, biggest threats are unplanned IT and Telecom Outage and interruption of utility supply, very low budget allocation for ITDRP, there is fairly performed BIA, and there is no end to end management support to warranty ITDRP implementation in Kenya's county. He has confirmed through his respondents that ITIL and COBIT are expensive which those could not be by the level of Kenya's counties because of they may not have capacity. Hence he came with simplistic and cost effective evaluative framework that ensures reliable assessment of the ITDRP plans in Kenya's counties.

The thesis presented by Berhanu (2017) was aimed to assess the practice of ITDRP. He has studied assessment of IT DR Practices in Ethiopian CBs. He intended to study the practice of ITDRP in 18 CBs of Ethiopia and found that 11 banks have IT DRP and 7 banks does not have ITDRP. His investigation shows that even the banks having ITDRP, the people tasks of ITDRP like testing the plan and updating the plan are identified to be components ignored by the banks.

Regarding alternate processing site, the use of cold site, hot site and warm site are put sequentially by his respondents. He assures that the Redundant Array of Inexpensive Disks system, cooling, power and connectivity redundancy, and virtualization constitute the top three system protection and resilience solutions have in place by the banks. He disclosed that none of the banks have considered international standards during ITDRP developments. Finally, he recommends that to address the observed gaps and weaknesses, the top management needs to regularly oversee implementation, update and testing of ITDR planning and preparedness in response to emerging threats. But he did not tell the management to apply which international standard, and did not inform to the technical how they should test and update the plan.

The work of Gerezgiher (2017) was focused on current status of ITDRP in banks. He has studied "An Investigation of Current Status of ITDRP in Ethiopian Banking Sector". His study has included 16 private and 3 governmental total 19 banks located at Addis Ababa and investigated either they have ITDRP or not. He found that almost

all Ethiopian banks are experienced on conducting AR and BIA in order to identify threats and vulnerability of their business contingency associating with their mission-critical services. In his study he explored that 11 of the banks have not a plan and 8 of the banks have a plan. He discussed that from the banks with ITDRP there is no bank which uses international standard of ITDRP application method. He recommended to use at least one international standard in their plan from ISO/IEC 27K series, NIST, COBIT or ITIL during implementation and post implementation of the plan. He showed that there is poor plan testing and updating. Even though he investigated from 19 banks 11 banks have no ITDRP and 8 banks have poor ITDRP, he lacks to explain why the banks have no ITDRP. Similarly, he did not propose the best ITDRP technique of testing and updating mechanisms.

The literature offered by Somasekaram (2017) entitled "A Component-based BC and DR Framework" was aimed to design, develop, and present a novel way of addressing the BC/DR gaps, while supporting the requirements of a dynamic IT environment. His analysis includes most existing IT frameworks including National Institute of Standards and Technology (NIST 800-34), ITIL, ITSCM, COBIT, ISO 22301, National Fire Protection Association (NFPA 1600) and Health Insurance Portability and Accountability Act (HIPAA). HE has employed design science research methodology. He wrote that although society thought that IT can operate without any problems, it is true that like other machines IT systems also is disposed to different failures. He concluded those catastrophes are grouped in to two known as inner and outer. Failure of server, storage, Central Processing Unit, data base or memory are inner disasters and externally created powers like heavy rains and flooding are categorized under outer disasters.

In his investigation he underlined that internationally provided IT standards are beginnings for a specific company to assess and investigate its gap and implementation depends up on the need and capacity of organizations. He has stressed that IT solutions must be protected from any blackouts by improving technical area of a company so as to provide best services. Finally, he developed a component based BC/DR which contributes software based solutions for IT companies. In his conclusion he showed, to get smooth and highly available IT services the company processes, procedures, and

policies managed by top managements must be ready to support to the recovery and BC operating team.

The previous literatures reviewed in this study showed that research on ITDRF has concentrated on the presence of the ITDR, creation of ITDRF for banks, developing evaluative ITSC/DRP for counties, developing ITDRPF for service continuity in smart city, assessing the practice of ITDRP and developing component based BC and DR for IT companies. However, based on the literatures analyzed this area of study still shows as little attentions has been given. Because there are areas which they need attention: Those includes; Separate ITDRF from BC with specific DR site type and investigation of maximum distance among main site and DR site. In Ethiopia there is no any available previous work which investigates ITDRF in any sector; and no previous work related to ITDR in telecom. This thesis summarizes the related works done in different sectors and were available publicly in diverse electronic repositories in the following table. The summary includes author name, title of work, date of publication, objective, applied methodology, findings brought, Proposed Solution/s and gaps which they have not addressed.

Author/s Name and year	Title of Work	Objective	Methodology	Findings	Proposed Solution	Gaps
(Uddin et al., 2015)	DR Framework for CBs in Sri Lanka	To develop a standard ITDRP framework for CBs in Sri Lanka	Qualitative Research	There is no standardized ITDRPF in CB of Sri Lanka. For that reason the use ad-hoc DR mechanisms.	The researchers have Develop a standard ITDRPF for Sri Lankan CB.	The proposed ITDRF was limited to CBs in Sri Lanka and other industries like airlines, telecom and other financial sectors were not considered.

(Hassan, 2017)	ITDRPF A study on IT Continuity for Smart City in Abu Dhabi Smart Government	To develop an ITDRPF for ITSC in Abu Dhabi Smart City	Quantitative Research	Thecomponents of ITDRPF for smart city were found to be implementation, continuity, people, technology, organizational and environment.	The researcher has developed an ITDRPF for ITSC by bridging the Gap between IT DRP components and Smart City components.	- The proposed ITDRPF was limited to Smart City of Abu Dhabi UAE Government and it does not explained the type of DR site that would be implemented with explanation of cases.

(Koech, 2016)	Evaluation framework for ITSC and DRPs: the case in Kenya's county governments	To identify relevant IT practices used and develop appropriate evaluative ITSCF for Kenya's counties.	Quantitative Research	There was no uniform ITSC /DRP evaluative framework among all counties of Kenya.	The researcher has developed a simplified evaluation framework for ITSC/DR for Kenya's counties.	- The evaluative ITSC/DR plan framework overlaps with BCP. - The framework was developed for counties of Kenya which has place restriction and it does not highlight systems level of importance.

(Somasekaram, 2017)	A Component-based Business Continuity and DR Framework	To develop a framework for BC/DR using a component-based approach.	Design science research methodology	There are either internal or external disasters happening in companies due to the absence of available BC/DR framework in their plan.	The researcher has developed a component based BC/DR framework in an application level.	The component framework for BC and DR has mixed some tasks of BC and DR each other. Since the study is concerned to all IT companies the financial capacity to implement DR is not included in the solution.

Table 2: Summary of related works from the reviewed literature

2.9. CONCEPTUAL FRAMEWORK OF ITDRP

Currently organizations of the world are reached at the level customer centric to provide services and products. The reason why is because of the increased multi-dimensional competitions among them. Due to the high race, companies are always in stress to become reputable and competent in the market. To get reputability and success, companies must work constantly without any service interruption. Since the advantage of using IT and telecommunications is get confirmed higher by every organization the e-service in general at this time is increased and dominant than ever before. So this Continuous Computing (CC) technologies are becoming standard frames of corporate level infrastructure set-ups. Similarly, IT and telecom services are critical for a company advancement. To realize that advancement creating accessibility of information systems in the company via different improvement mechanisms like BCP and DRP and managing mission critical, business critical and corporate through a scientific frame is mandatory.

So irrespective of size any IT company thinking to have a DR must firstly perform RA for the existing information technology resources. In doing the RA there should be filtrations of the type of systems either mission critical, business critical and normal. Then there should be investigations of networks resources and its desirable amount for maintenance in daily activities. Next to resource analysis action plan should be followed by integrating the plan with the company business strategy. In this stage company must fix the type of ITDR site to be owned, the maximum distance among the live systems and the ITDR system, the type of ITDR setup either active-active or active-stand by and the functioning departments. After that human resources of the company must include the ITDR training program for employees with in its specific plan.

Then the company should go for implementation stage by providing training for employees relevant to specific tasks to be accomplished by individuals including their level of involvement and the way how and with whom they should perform the tasks. For implementation strategies company must incorporate and forced to the team to perform different imitation disaster scenarios at least two times a year with in six years' interval. This mock disaster presentation will certify and upgrade skills of individuals for the time of disaster. The three ITDRP development procedural phases (construction,

adoption, and evaluation) must be countered. Starting by construction phase (concepts and thoughts must be changed to concrete activities). Then the ITDRP team should be created which contains members from all concerned departments. Again this filtered team must perform RA for all functioning areas of the company in order to show the severity of disaster in company mission critical and business critical systems if it happens. After completing the risk analysis and showed the levels of importance having an ITDRP in a company the team must present a workable action plan to the top management asking for endorsement.

Management can be challenging for easily approval of adopting ITDRP, but the team must be very strong and expressive in the risk analysis presentation with internationally reported disasters due to different things. After the approval of management ITDRP is adopted and incorporated in to the organizations day-to-day business tasks. In this phase tasks like creation of awareness for staff, announcement of internal communications among the concerned members, exchange of job descriptions, training schedules and the level of follow up, incorporation ITDRP in to daily operational procedures, informing reporting phases, ITDR handling processes and procedures.

The ITDRP committee must perform tasks based on the provided plan and at the time of necessary actions need to be accomplished the team must go with no ignorance of activates out of the plan for company guarantee. After the adoption of ITDRP and its incorporation with daily operations management must follow and support the team by performing regular evaluations and gap analysis for improvements. If the company changes or adds new systems, new servers, storages and other supporting machines the plan must be updated and evaluated in the perspectives of mission critical, business critical and normal and then incorporate as its necessity in to the ITDRP. To improve and upgrade necessary solutions to the plan, the roll of top managements by providing necessary evaluations in terms of testing the plan, updating, the plan, monitoring different operations and taking important trainings is very critical concerns.

2.10. ITDR FRAMEWORK DEVELOPMENT FOR ETHIO TELECOM

Ethio telecom is a monopoly telecom service provider in Ethiopia. Since the company is working to be a world class telecom operator, it must fulfill different required standards of IT services like warranty of company ITSC and data protection at a time of disaster. As the information gathered at the time of preliminary study it showed that the company has no ITDR in place. The reasons are lack of organizational culture, lack of support from top management to have DR site, lack of availability of clear and workable framed plan for ITDR, poor financial and resources auditing, absence of accountability from top management to lower staff, absence of contestant/competitor in the market, absence of challenging teams in the company and lack of thought to stay in the company.

Though the company is challenged by different disasters it still ignored to think about it. Currently there are disastrous issues in ethio telecom like loss of critical data, repeated service interruptions, hardware and software related failure; due to that there is increased cost of down time reported by different local and international mass Medias. IT and telecom service dependent companies placed in Ethiopia are always unsatisfied on the services delivered by ethio telecom. These problems are born from service interruption due to lack of improved and reliable DR site.

According to (Hawkins et al., 2000) having DR is equal to implement company insurance policy. (Uddin et al., 2015) added organizations must be conscious to think about dangerousness of black outs and get ready to cope up from that blackouts. As (Koech, 2016) said by referring to Gartner and Holub (2015) “in developing IT excellence, organizations pursue IT operation optimization through implementation of established frameworks in five principles listed as follows”:-

A. Strategize and Plan - Draw Charters to synchronize with vision and align with business goals.

B. Develop Governance - Establish decision making channels and agree on flow.

C. Drive change management - Get buy-in from stakeholders.

D. Execute - Optimally operate in accordance with business objectives.

E. Measure and Improve - measure outcome, seek feedback and drive improvement processes.

The preliminary study of this thesis approved that there is no financial problem to rollout ITDR for ethio telecom rather the human element of the company is unorganized and not maturely thinking about readiness of DR.

Combining the information gathered from the preliminary study and literature review of this thesis; the researcher proposed an ITDRF for ethio telecom. The first point in the frame was that ethio telecom should include ITDR in its BCP and operationalize it by avoiding all the human element challenges to launch ITDR for the company. To minimize and totally eliminate human ignorance to ITDR performing reliable training and experience sharing starting from top management to concerned IT staffs. The ITDRP operations must be included in company IT operation tasks and should be managed under IT operations director ecosystem. After arranging this the company can deeply immerse to think and realize the following three areas; Select Appropriate Technology, Setting Up Secondary DR Site and Design of facility (Uddin et al., 2015).

1. **Select Appropriate Technology:** According to (Swanson et al., 2010) data should be frequently backed up in a clearly definite rule usually based on criticality. Doing task of BIA again to separate the critical systems and applications based on their sensitivity. Top five very important approaches of back up are discussed for this research as follows.

A. Metro Cluster: A high-availability solution, installed in the same urban area.

B. Fast Restore: A high-availability solution usually accomplished within same DC.

C. Application-Level or Middleware-Level Clustering: Clustering is a good solution to attain better high-availability need, but it is not a solution for physical disasters.

D. Application Data Mirroring: This is a DR method which works by real-time replication of data bases of applications. And it is recommendable as a DRP technology.

E. Disk Mirroring: It is part of every business application currently and it is a good solution to continue business by overcoming disc level failure. But, this does not provide support if there is physical disaster or full system blackout.

2. **Setting Up Secondary DR Site:** ethio telecom must have DR site operated by its own staff members without outsourcing for the operational activities and location should be in its own place in Ethiopia where DRP requirement fit area (in terms of freeness from any known natural disasters, far from airlines landing, far from commercial power distribution over cross, easiness of getaway access connectivity, far from main roads and unsunny weather, distance maximum 150km, minimum 50 km not with in the same city).

3. **Design of Facility:** Since ethio telecom has very critical applications and data active- standby (hot site) is recommendable considering all mission critical number one and all mission critical number two systems readily available at the DR site, real-time replications of databases, similar applications and similar infrastructure must be launched to get infrastructure support for a low RPO which is 10 minutes and RTO of 12 hours. Data replication depends up on the criticality and of the data. Two copies of physical tape media stored one in primary site and the other one in DR site must be incorporated as a mandatory need. Considering this the following framework is proposed for ethio telecom ITDRP setup.

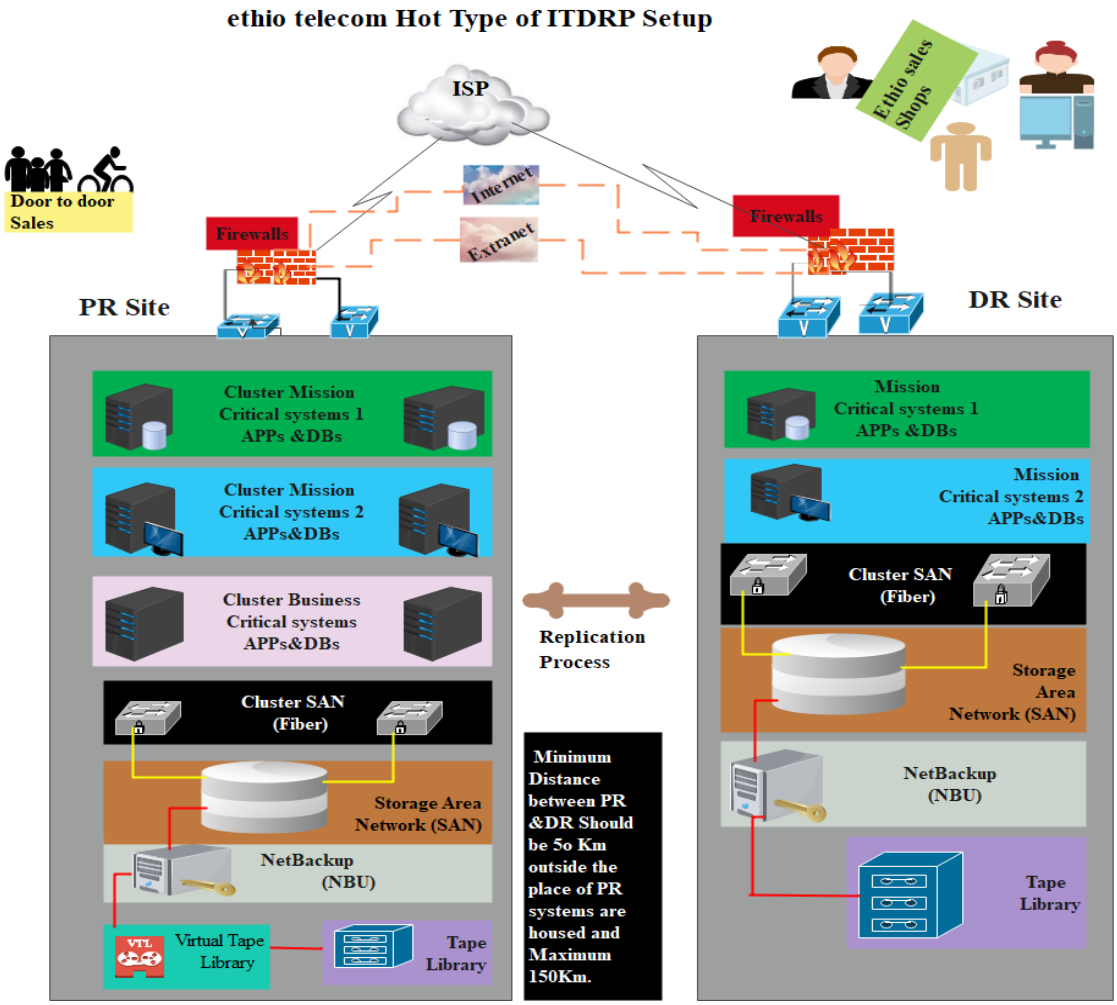

Figure 7:Conceptual ITDRF for ethio telecom (adapted from Uddin et al., 2015)

2.11. CHAPTER SUMMARY

Literature review part of a thesis is knowledge scanning and skimming, widening, summarizing figuring and grasping section of a whole thesis. The chapter has five cascading. The first cascading presented introduction. The second section discussed about definitions of disaster. It was clarified terms, definitions and meanings of disaster, IT disaster, IT DR and IT DR framework. The third cascading focused on detailed penetrations of the notion ITDR, highlighted on ITDR framework challenges and ways to overcome those challenges. The fourth portion presented some pertinent previous works related to ITDR framework. The fifth section presented the conceptual knowledge and the proposed framework for the selected company (ethio telecom) based on the knowledge gained of the review. Through this cascading there are many

important findings achieved. The findings are presented here in the following paragraphs.

First finding is discovery of IT companies could have one type of ITDR site; from the six types of DR site types called hot site, cold site, warm site, mobile site, mirrored site and winging site depending up on their business requirements and financial capacity. Second finding is investigation of challenges to develop ITDR in organizations. Those are top management support ignorance, lack of sufficient financial aid, absence of alignment between ITDR objectives with business goals, absence off-site backup, problem of choosing correct alternative site, difficulties of maintenance and update of ITDRP, lack of continuous testing of ITDRP, shortage of adequately trained staffs working on ITDR and absence of doing RA and BIA. Third the findings of necessary elements to develop ITDRP. Those elements are people, process, technology and infrastructure. From those important elements the three (people, process and technology) were found to be famous and infrastructure was found to be included under technology.

The objective of the review was to find out the most important unified strategies that support by unifying detail activities in a model format to develop ITDR framework. And that framework fully leads to a formal integrating tool for telecom ITDR establishment in an agreed manner. Findings from the literature review shows that four important things must be performed to develop ITDR. Those includes fixing the type of ITDR what type it should be depending the organization's financial capability, minimize challenges of developing ITDR, performing RA and BIA activities and lastly know the necessary ITDR elements.

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1. CHAPTER INTRODUCTION

In many different writings the words methodology and method are used interchangeably. But the fact from professionals and scholars put in ground does not support to use them as equal and the same. According to Oxford Advanced Learner's Dictionary, 8th edition (Hornby A., 2010) methodology is "a set of methods and principles used to perform a particular activity" and Method is "a particular way of doing something".

In addition to (Goundar, 2012) provided a that "Research methods are essentially planned, scientific and value-neutral various procedures, schemes, algorithms, etc. used by a researcher in a research. Research methodology is a systematic way to solve a problem. That includes procedures by which researchers go about their work of describing, explaining and predicting phenomena. It is also defined as the study of methods by which knowledge is gained." Research method is a means to get information from the sample while Research methodology is way of attacking problem by applying the information get via research methods (Grover, 2015).

(C.R.Kothari, 2003) explained the difference between the two terms as follows "Research methods may be understood as all those methods/techniques that are used for conduction of research. Research methodology is a way to systematically solve the research problem." As (Rajasekar, 2018) said *r*esearch methodology is a systematic way of solving problem there by describing, explaining and predicting phenomena aimed to provide plan of task in the research being conducting. According to Mishra (Mishra & Alok, 2017) research methodology is a science of investigation for ways on haw research can be systematically conducted. With these different scholars' idea in mind this methodology section of the thesis presents the specific ways how data is gathered, analyzed, discussed, presented and confirmed its validity & reliability. In general, the chapter offers the combinations of specific methods & principles (methodology) applied with in the entire thesis.

3.2. RESEARCH DESIGN

According to (Yin, 2014) research design is the over-all system of how a researcher will approach his/her research question. It is a linking point for the collected data and conclusion brought to the study question set in the primary step. As (Akhtar, 2014) described, research design is a fasten which holds all of the elements in a research project together. It is a plan that identifies the homes and category of data pertinent to the research problem, a strategy identifying which approach perfectly be used to gather and analyze data and visualize the time & cost budget constraints. Akhtar underlines that a research design should be able to clearly show answers of inquiries like what is the study about, what type of data is required, purpose of study, sources of needed data, place or area of the study, approximately required time for the study, amount of required materials for the study, type of sampling applied, what method of data collection was applied & appropriate, how data is analyzed, approximate expenditure and specific nature of the study.

(Ridder, 2017) has put that in qualitative study the most known and common designs are case study, ethnographic, grounded theory, narrative, phenomenological, action research. To apply those designs in a separate mood depending research type researcher must understand his/her study type. Researchers apply case study to examine an in-depth truth depending occurrence having an exact outline brought from primary or secondary qualitative data gathering mechanisms for the purpose of pattern discovery which affect an occasion.

Ethnographic research is applied in a separated area for a selected or specified culture by providing much amount of time to confirm a perfect sample having specific factors about a wider population (Van Hulst et al., 2015). The researcher explored ITDRP framework not detailed culture of a given community; hence ethnographic research design was not appropriate for this study.

Investigators apply a grounded theory research design aiming at formulating and building new theories than empirical testing of the theory depending on gathered data in developing social progression under a given field (Khan, 2014). Since the researcher

did not assess a social process & action or there is no developed theory by the researcher, grounded theory research design was not suitable for this study.

A narrative researcher design is employed by researchers aimed to examine stories to discover and understand people, culture and societies. And it investigates complications of human practice depending on story of individuals private know-how (Wolgemuth & Agosto, 2019). The researcher did not discover a personal experience, nor was gather written narratives for that matter narrative research design not applied in this study.

Phenomenological research design is applied by investigators aimed to investigate participants lived experience (Umanailo, 2019). A researcher can use a phenomenological research design to recognize lived events as represented within a Knowledge base of an explicit phenomenon (Qutoshi, 2018). Phenomenological research design was not appropriate because the researcher discovered participants' current experiences on ITDRP related activities in the company ethio telecom not about lived practices of a specific phenomenon of occurrence.

Action research is applied by researchers intended to upgrade success and effectiveness of people on their personally involved areas of job (Burns, 2015; Nicodemus, B., & Swabey, 2015). The investigation of this study did not concern to upgrade personal achievements of individuals on their engaged work. So the researcher did not apply action research methodology because of it is not appropriate for this study.

Researchers select a case study research approach when their purpose is to investigate and explore an existing issue in an empirical way from up to down with in factual life (Yin, 2017). It was with this logic the researcher selected case study approach needing to employ an in-depth investigations of an issue, event or phenomenon exist in the case company ethio telecom regarding to its ITDRP applications.

3.3. SINGLE CASE STUDY RESEARCH DESIGN

As (Solomon, 2018) defines case study by citing Robson "a strategy for doing research which involves" an empirical investigation of a particular contemporary phenomenon with its real-life context using multiple sources of evidence". A case study approach

offers tools for researchers to investigate complicated cases or phenomena inside their settings (B. Pamela & Jack, 2008). (B. Pamela & Jack, 2008) said researchers apply case study approach when they ever need to look at detail interactions with in its context. Also it is help full to study a particularity and complexity of a single case using case study (E.Stake, 1995).

In this study the researcher aim was to conduct an in-depth investigation about the ITDRP situation in ehtio telecom, hence to discourse the research questions and achieve the study points the case study design was got fit for this research paper and researcher has applied it. The case study approach was resonated as trying to recognize the encounters that impact on achieving an improved ITDRP. Yin classifies case studies as explanatory, exploratory, or descriptive. He similarly separates between single, holistic case studies and multiple-case studies.

Stake categorizes case studies as intrinsic, instrumental, or collective. (Yin, 1984) declares that based on design there are four case study types: embedded, holistic, single case and multiple case. He also added that holistic and embedded designs have other classification types called: type 1 single case (holistic), type 2 single case (embedded), type 3 multiple- case (holistic) and type 4 multiple-case (embedded). In addition to other scholars classifications of case study, (B. Pamela & Jack, 2008) also provided similar categorizations with Yin that case study researches depending their purpose are classified as exploratory, explanatory, descriptive and confirmatory. (Rebolj, 2013).

Holistic designs (Single case type 1&2) investigates the case in two ways in single unit of analysis within a single case designs and embedded designs investigates the case in a multiple unit of analysis within single case designs. The purpose is to study serious established present theory, uncommon situations and symbolic case regarding to a single case design. Multiple case (type 3&4) also has two dimensions called holistic designs investigating the case as single-unit of analysis within multiple case designs and embedded investigating the case as multiple units of analysis within multiple case designs; the purpose is to perform comparative investigations. The below figure highlights the 4 categorization of case study research design.

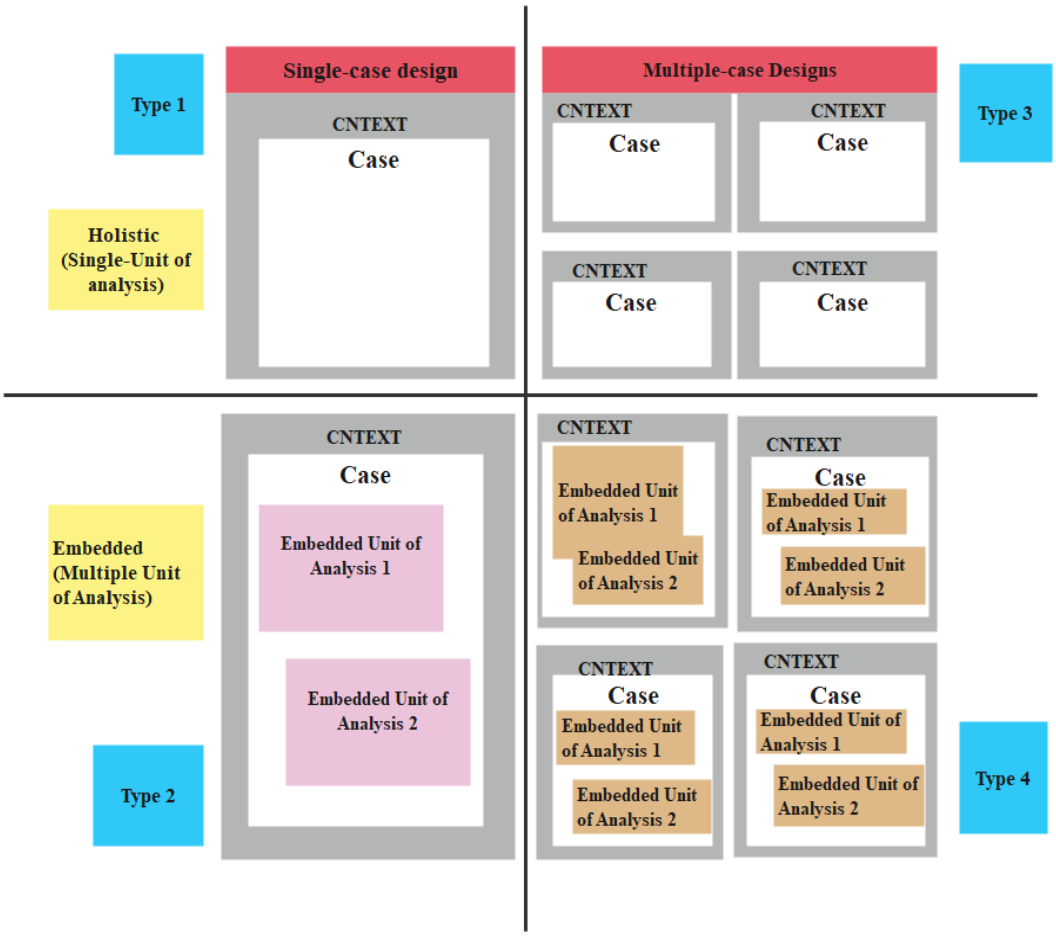

Figure 8: Illustration of holistic and embedded research designs under single case and multiple case (Reprinted from slide share.com)

For the purpose of this study the research chose single case design with holistic (single unit of analysis) case study type1, because there were not cases to be studied comparatively. Describing the current phenomenon and proposing solution was primary aim of this study; hence the real situations of ITDRP in ethio telecom with examples and evidence was presented in an in-depth way under the statement of problem of this study. Therefore, single case design qualitative approach was appropriate and applied by the researcher. The below figure represents the case study design employed in this research paper.

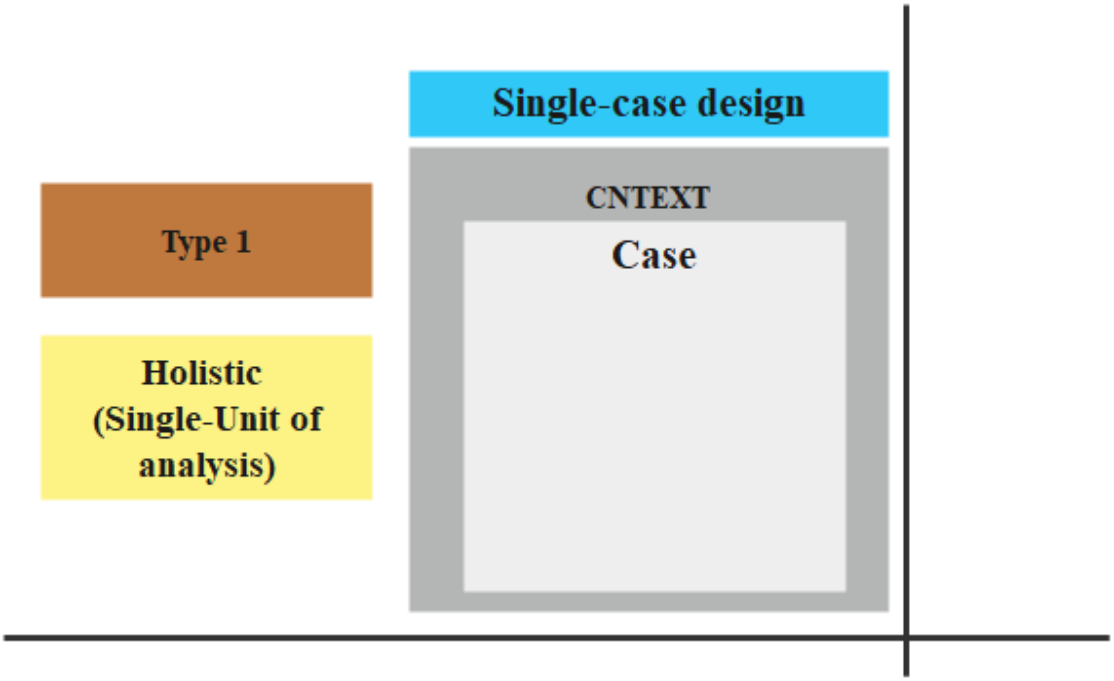

Figure 9: Illustrates single case design (adapted from Solomon, 2018 p.53) strates single case design (adapted from Solomon, 2018 p.53)

3.3.1. UNIT OF ANALYSIS AND UNIT OF OBSERVATION

According to (Dolma, 2009) the term unit of analysis is defined as "the entity that is being analyzed in a scientific research". Unit of analysis is the major entity that researchers are going to analyze in their study. Those units can be individuals (like a school director, or someone who has knowledge of an area), groups, artifacts (books, photos & newspapers), geographical units (town, census tract, state), social interactions (dyadic relations, divorces & arrests) (Li et al., 2017). Solomon (2018) cited Yin (2009) and put that "the unit of analysis is the basis to the fundamental problem of defining what the case is". He added that the units may be single person, or an occasion/object (such as a decision, a programmer, process in organization/s or change in company), or an institution or group or department/section in an organization. In short unit of analysis (a case) is a level at which researchers reach their conclusions.

(Sedgwick, 2014) states that the unit of analysis is defined statistically as the "who" or "what" for which information is analyzed and conclusions are made. As (Kumar, 2018) explained there are almost endless diversities of possible units of analysis in different researches, however the most common ones are individuals, group, organizations and social artifacts & social interactions.

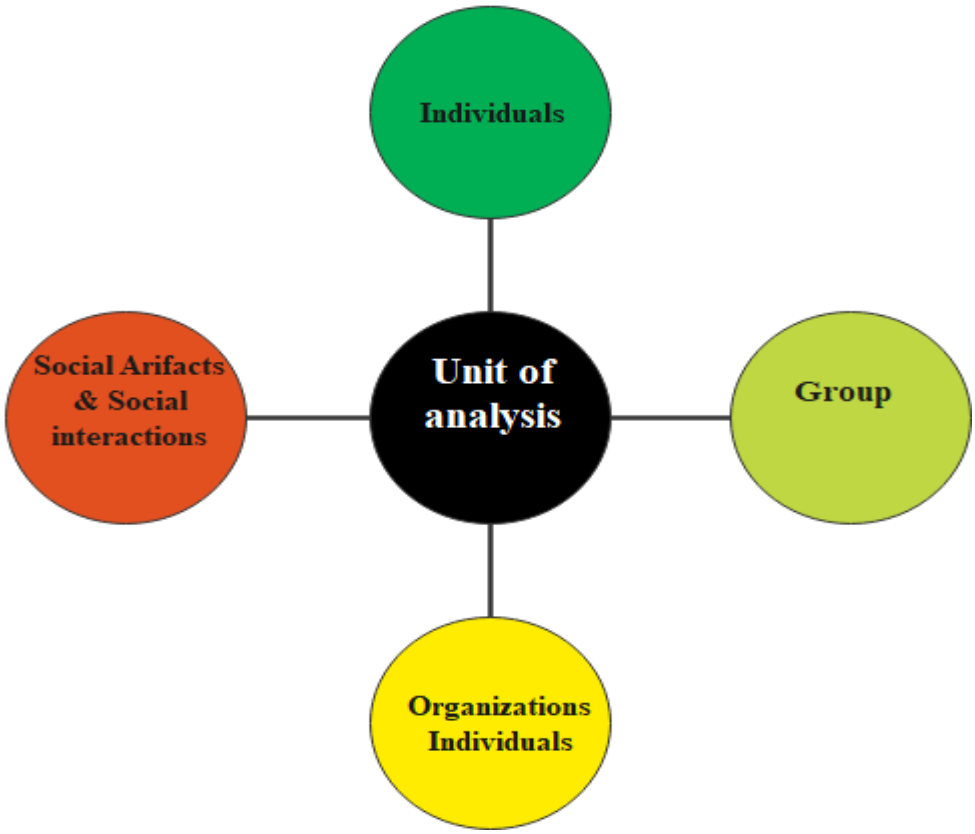

Figure 10: Classifications of unit of Analysis (Adopted from Kumar, 2018 p.72)

Any researcher in any field of study must consider the unit of analysis in research deign so that to refine every important elements of a research (Paré, 2004). When unit of analysis is not clear to researcher, s/he cannot: (explain the research problem, make hypothesis, decide sampling method, select the right measuring instrument for data collection, decide valid data analysis option and finally generalize the results to a population). And finally her/his whole study work will become in a risky condition. Unit of analysis touches and influences each component of the study development. Therefore, defining the unit of analysis has a significant part in any research development. Unit of analysis call by researchers such as individuals, a process or social artifacts is worthless; however, the worthwhile is clarifying about what the researcher's unit of analysis is about. Researchers at a time of conducting research work must select either researcher is investigating managerial skill or managers, supervision or supervisors, corporate sector or corporate administrators (Kumar, 2018).

While researchers are bearing in mind what their research questions will be, they have to too fix what the case (unit) is. In order to get supported to determine what the unit is, researchers should ask themselves the following questions: "What my case is; do I want

to “analyze” the individual? Do I want to “analyze” a program? Do I want to “analyze” the process? Do I want to “analyze” the difference between organizations?” answering those questions with friends and coworker could be best way for further demarcation of research unit (B. Pamela & Jack, 2008). For example, the question might be, “How do women in their 30s who have had breast cancer decide whether or not to have breast reconstruction?” In this example, the case could be the decision making process of women between the age of 30 and 40 years who have experienced breast cancer.

However, it may be that you are less interested in the activity of decision making and more interested in focusing specifically on the experiences of 30-40-year-old women. In order to extract unit of analysis for this case study similar theoretical framework researches must be assessed. In the first example, the case would be the decision making of the group of women and it would be a process being analyzed, but in the second example the case would be focusing on an analysis of individuals or the experiences of 30 year old women (Kumar, 2018).

Similar to the example presented by Kumar the researcher has reviewed several peer-reviewed literatures which could be put as identical conceptual framework. Considering this notion this investigation uses the work of Mueen Uddin, Sandun Hapugoda & Roop Chand Hindu (2015) as a similar conceptual framework. Accordingly, the main unit of analysis for this investigation is an implementation process of ITDRP framework in the entire company of ethio telecom and the minimum unit is the individual staff working in information systems and information security divisions.

The unit of observation also called measurement, is explained statistically as "who" or "what" for which data are measured or collected (Sedgwick, 2014). Unit of observation refers to the entity at which measurements are done and the level at which data in a research is collected. Unit of observations could be individuals, families, documents etc (Kumar, 2018). In this study the unit of observations were the individuals in different levels and documents from different departments of sections.

3.3.2. PARTICIPANTS SAMPLING TECHNIQUES

Sampling in research could be either probability or none probability sampling (Sarstedt et al., 2017). To reach at an accurate conclusion depending on the gathered data from

respondents researchers must choose appropriate representatives to their research problem (Hennes, 2017).

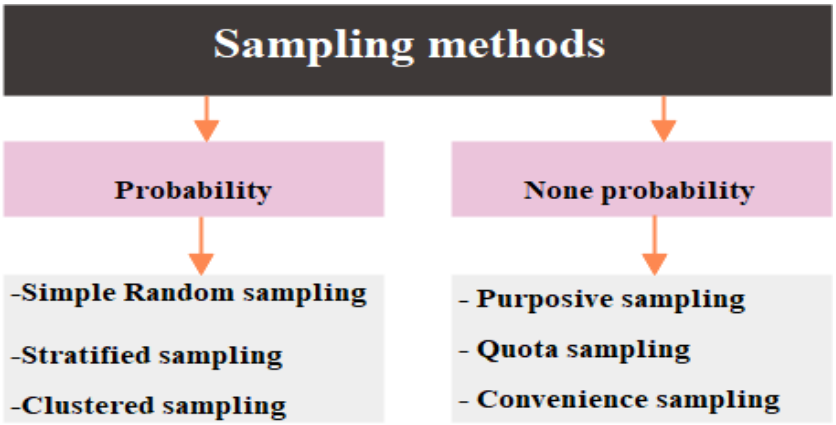

Figure 11: Basic sampling methods (Adapted from Sarstedt et al., 2017)

According to (Elmusharaf, 2012) research sampling in qualitative research approach is performed consciously. This research employed none probability purposive sampling technique as the need of the researcher is in depth investigation about the mater from well experienced and highly skilled staff members. Since participants are selected reasonably relying on their experience, position, relevant working skill and others thoughts the method is data reduction (Hoeber et al., 2017). As researchers thought that participants have enough information about the matter and apply purposeful sampling the information about a particular phenomenon under investigation becomes maximized (Hayes et al., 2017).

Researchers who employ purposeful sampling uses their top decision making to choose appropriate contributors for providing information on the case selected for study. And s/he uses purposeful sampling to certify appropriate data collection for the conduct of rigorous investigation (Gerassi et al., 2017). In order to find more theme interview of 16 contributors is sufficient after grasping data saturation (Namey et al., 2016). However, for the purpose of categorizing strong synopsizes through a given and reach at data saturation many researchers still use 20 to 40 interviewees (Julie et al., 2018). When researchers thought further data collection is unnecessary, data saturation is approved(Benjamin et al., 2018).

The researcher approved that data was saturated after gathering data from the initially conducted 18 respondents which means 72% of the participants. Because the rest 7

respondents or 28% of the participants did not add any additional significant information exceeding the former 18 contributors. However, it was the need of the research to conduct the interview session with the 7 respondents supposing there will be new additional information.

Respondents were purposefully selected by considering that the divisions, departments and section who they belonged to are roots of the organization by handling different strategic, deployment, operational and security related activities.

For this research study the researcher used purposeful sampling to achieve the sample of 4 directors, 6 managers, 6 experts, 4 supervisors and 5 specialists in total 25 participants of IT professionals from two divisions (Information Systems & Information Security) of departments and sections. The reason is that those samples were from the critical functional areas who they directly concerned to the case investigated. Respondents were selected on the basis of preset eligibility criteria from both IS and ISec divisions.

3.3.3. CONTRIBUTORS ELIGIBILITY CRITERIA

To select participants purposefully; the researcher employed some eligibility criteria that respondents must own to be part of the study. The criteria used for participants' eligibility approval were listed as follows: -

1. Respondents with minimum of five years' work experiences under IS and ISec divisions of departments
2. Respondents with relevant work experience under IS and ISec divisions of departments and sections.
3. Respondents working as one of the succeeding titles specialist, supervisor, expert, manager or director under IS and ISec divisions
4. Voluntariness of interviewees after researcher explained the purpose of the investigation to be part of the study

Restricting time frame was decided by the researcher depending on the company motivation and appraisal strategy so as to ensure acceptable experience in IS and ISec related activities. So respondents with single fit criterion, double fit criteria and triple fit criteria were not eligible for this study.

3.3.4. DATA COLLECTION TOOLS AND TECHNIQUES

As (Elmusharaf, 2012) has written in his article, in qualitative research approach the common means of data collection are interviews (Semi structured interview, structured interview, unstructured interview) , focus group, document analysis and observation. This research study applied two data-collection methods; interview (semi-structured) interviews and document analysis. The data collection process applied in this research study had two steps presented as follows:

Step_1. The directors of Risk & BC, IT strategy, IT design, IT transition, and IT operation departments were requested to give permission to the researcher to perform document analysis on the current documentation on organizational BC/DR, service continuity monitoring, and current practices of data backups for the ITDRP document analysis.

Step_2. Conducting the semi-structured interview questions with twenty-five (25) individual of IT strategy, IT design, IT transition, IT operation and IT security Risk department directors, section managers, experts and specialists. This process excluded the researcher who is a specialist in one of the IT transition department sections.

3.3.4.1. DISASTER RECOVERY PLAN LITERATURE REVIEW AND DOCUMENT ANALYSIS

Irrespective of discipline, developing research and connecting it to existing knowledge is the problem of all academic research activities (Snyder, 2019). Literature review in different sectors like county services, banking, smart city and small & medium organizations was performed and the existing knowledge was used in the semi-structure interview question development as initial knowledge constriction. Since qualitative research requires dynamic data collection techniques literature review and document analysis contributes a lot by approving some or all of the following advantages (Bowen, 2009; Snyder, 2019). The advantages include: - Providing background information as well as historical insight, enabling situations that need to be ask questions or observe as part of the research, providing supplementary research data, providing a means of following change & development and Verifying findings or validate proof from other sources.

According to (Bowen, 2009) document analysis is one of the main data sources usually used in qualitative case studies. Document analysis regularly is joint with other qualitative research approaches to attain triangulation. For this study it elaborated the collection and examination of current records or documents on ITDRP and data backup mechanisms and experiences in the company ethio telecom. The BCP/DRP document analysis was used to collect important evidence and knowhow of current BCP/DRP documentation in the company and hint of how ethio is involved with ITDR.

The document review of policies, organizational plans and DR practices in the company provided value to the research by letting the researcher to control how DRP is perceived from a strategic and operational viewpoint, and to triangulate data collected through the semi-structured interviews. Therefore, it helped in the identification of significant patterns and themes. Documents included in the analysis were; previous years' practice related to Disaster and DR tasks, Strategic plans, Operational plans, Risk management policies, procedures and practices, BC policies, procedures and practices and learnings from past disastrous events.

3.3.4.2. PROCESS OF SEMI-STRUCTURED INTERVIEWS (SSI)

In this section the researcher presented all the activities conducted to collect the empirical data. Semi-structured interviews (SSIs) are excellently suitable for a number of important activities, specifically when there are open-ended questions requiring follow-up enquiries (Adams, 2015). Especially cons in the following circumstances:

- If researchers need to ask probing, open-ended questions and want to know the independent thoughts of each individual in a group
- If investigators need to ask probing, open-ended questions on topics that your respondents might not be candid about if sitting with peers in a focus group
- If you need to conduct a creative program evaluation and want one-on-one interviews with key program managers, staff, and front-line service providers
- If you are examining uncharted territory with unknown but potential momentous issues and your interviewers need maximum latitude to spot useful leads and pursue them

(McIntosh & Morse, 2015) the SSI is designed to determine subjective reactions of individuals about an event, situation, phenomenon or happenings they have experienced by employing a detailed interview guide. For this study purposive semi-structured interviews were considered as one of the most suitable technique as the method enables researchers to get richer data from opinions, practices, procedures and day to day operational activities of selected individuals.

This nature of the method let the researcher to employee it into the data collection method get rich data from the selected contributors. Open ended and flexible method creates idea exploration about the matter under investigation. Hence, pre-arranged guiding questions was set and conducted an interview with the contributors according their conducive time. The interview was not conducted simply. It was challenging and time taking as both researcher and contributors were afraid of the pandemic COVID-19 it was really 'really' very challenging and difficult to get interested participants. And sometimes arranged plans and programs were not kept by respondents as all staff were not attending work place researcher was obligated to wait until the time respondents come to office.

The semi structured was performed via two modalities called face to face and over the phone. According to (E.Stake, 1995) interview setting should be secured and must be employed on the choices of respondents; collecting, de-identified and anonymous data is recommendable to achieve security of respondents. Researchers should not collect any information that can easily identify a respondent. In addition to collection of data writing the report also needs carefulness not to expose participants' security and keep the consent deled with researchers.

This study was applied based on the agreement of respondents for interview place, time, the recording tools and sharing of supporting documents they have at their hand. The researcher arranged different time based on contributors' agreement. Though it was challenging the method allowed each participants to follow their individual path and accounted them in each circumstance or context. The application of semi-structured opened ended questions supported to realize an explanatory study which allowed for cases to arise from the participants, availing vision into the outlooks and personal view & understandings.

As (Hoepfl, 1997) presented by citing (Strauss and Corbin, 1990; Patton, 1990) there are some principles and guidelines to be consider at a time of preparing semi-structure interview questions. Those key guiding questions are: -

1. Feeling questions planned to understand the emotional responses, participants have to their know-hows
2. Knowledge questions relating to factual information the participants have
3. Background or demographic questions concerning the identifying characteristics of the participants such as age, occupation and education
4. Thoughts or value questions intended to understand the participant's interpretive and cognitive processes
5. Experience or behavioral questions relating to what participants do or have done
6. Sensory questions about what the participant has seen or heard

The researcher also followed those experiences of guidelines and best practices to prepare the semi-structured questions. The application of this method benefited to the researcher from its flexibility & openness to go and create continual inquires for cases thought that researcher needs more attentions. The method supported the researcher to shadow an in-depth vision in to more specific & exact arguments. The interview execution was performed in face- to- face and over the phone channel. All face to face interviews with individuals was consumed maximum of 90 minutes & minimum of 55 minutes.

The interview held with 12 contributors consumed each 90 minutes and with those of 8 contributors consumed 55 minutes each. In average the face to face interview with total of 20 contributors consumed 76 minutes per individual which mathematically calculated as follows. (12*90) =1080 + (8*55) =440. (1080+440) =1520/20=76 minutes. The interview of 5 contributors was conducted over the phone and consumed different duration of time. The session (with 2 contributors each consumed 40 minutes and with 3 contributors consumed 30 minutes each) in average 34 minutes per individual was conducted; which was calculated as (40*2) =80 minutes and (30*3)=90 minutes, 80+90=170/5=34 minutes. The language used for interview in both modalities (face to face and over phone) was local language (Amharic) and the interview data was selectively recoded according the consent of the participants. And the recorded and

written data in Amharic language was transcribed, and participants were given fictitious name (coded name) in the transcriptions so as to separate respondents from other respondents.

No	Respondents Category	Number of Respondents
1	Directors	4
2	Managers	6
3	Experts	6
4	Supervisors	4
5	Specialists	5

Table 3: Illustrations of interviewee distribution across their hierarchy

Seeking for in-depth investigation, the researcher agreed with respondents using informed consent. Informed consent is a voluntary agreement to participate in a research by providing information relevant to the study area (Hagemann et al., 2003). To get an in-depth response from respondents the researcher applied an attempt of joining and associating research questions with interview questions. Planning to meet with respondents was one of the most crucial task to collect data from the volunteers. However, in this study, since the contributors and researcher were participated in at their spare time there was no permanently fixed time table rather we use flexible contact time to meet each other. This is part of maintaining respect and smooth relationship with contributors.

A drafted plan with list of divisions & departments of contributors was used as a remaindering time table which it looked like as printed here under in the table.

Mode of interviews	Divisions	Departments	Contributors Position					Scheduled Time	
	Information Systems		**Director**	**Manager**	**Expert**	**Supervisor**	**Specialist**		
		IT Service Strategy		1	1		1	March week 4	
		IT Service Design	1	1	1		1	April week 1 and 2	
		IT Service Transition	1	1	1		1	April week 3 and 4	
		IT Service Operation	1	2	2	4	1	May week 1,2,3 &4	
	Information Security	Risk & BC	1	1	1		1	June week 1& 2	
			4	**6**	**6**	**4**	**5**	Total	
			25					**G. Total**	
Face to			4	5	4	3	4	**20**	Total
Phone			0	1	2	1	1	**5**	Total
								25	**G. tootal**

Table 4: Contributors working department, flexible time table and mode of interview

Semi-structure interview had its own procedures; the bold steps and processes applied in face to face semi-structured interview was presented here under the below figure.

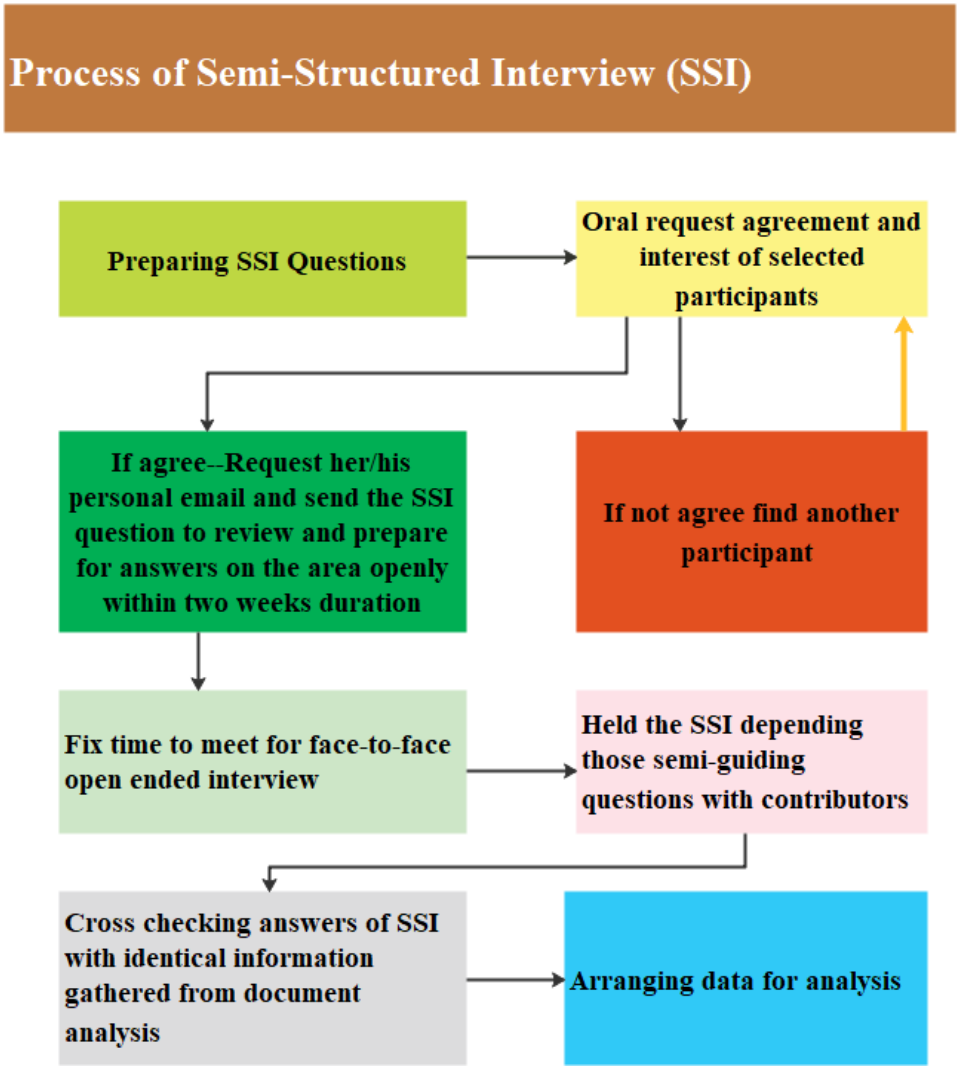

Figure 12: Process of semi-structured interview

3.4. DATA ORGANIZATION TECHNIQUES

The data collected from documents analysis & semi-structure interviews was organized as much suitable for analysis as the researcher need. According to (Regmi et al., 2010) interview data for research should be transcribed and labeled. The researcher transcribed the semi-structured interview data from Amharic handwritten hard copy & audio recordings to word softcopy document by making fictitious name instead of real respondents' name. Researchers must kept their data securely in either or all of the following securing methods: encryption, (device level inscription or data level inscription), secured cloud storage and securing access (O'toole et al., 2018). The researcher had put all data securely by creating strong password per device level and file level.

For the device level flash disk is password protected and kept in secured place at researcher's home and office in different flashes with lockers only accessed by researcher; for the file level all collected data were password protected and put in different cloud storages account of researcher (Dropbox and Google Drive). After data is collected from different sources it should be organized in any of the following five data organization options include: location, alphabetical organization, time, hierarchy and category. For this research study the researcher organized the semi-structured data collected from respondents by categorization option as helpful to analysis as possible. The steps employed or semi-structured data organization was presented below in figure.

Figure 13: Process of semi-structured data organization

3.5. DATA ANALYSIS

Data analysis a way of minimizing huge amount of collected data to make sense of theme (Kawulich, 2004). Barbara Kawulich added the idea that to analyze data three things occurred namely: data are organized, data are reduced through summarization and categorization, and patterns and themes in the data are identified and linked by referring Patton (1987) in her article. For this research study the research presented all the steps and beyond that in the data organization as it is presented in the previous page. There are a number of data analyzing techniques qualitative case study approach including the five techniques read by Yin (2003): pattern matching, linking data to

propositions, explanation building, time-series analysis, logic models &cross-case combination (E. B. Pamela & Jack, 2008). Even though there are many ways of analyzing qualitative data which beginner researchers become overwhelmed by the numerous techniques; they need to know that there is no agreed way to address the method (Kawulich, 2004).

Understanding analyzing strategy is better than relying on analytic tools: It is clear that computer assisted analytical tools for qualitative study are useful when the case to be analyzed is clear for the researcher. If researcher still is unclear what notion and with what notion to analyze, using the tools is meaningless (Yin, 2017). Yin added that the purpose of the analytic strategy is to link researcher's case study data to important concepts of interest, and then to have the concepts give you a sense of direction in analyzing the data. There are four general strategies of data analysis namely: relying on theoretical propositions, working your data from the ground up, developing case descriptions, and examining rival explanations but are not limited you can develop your own strategy also. The researcher applied the working your data from the ground up strategy of data analysis with additional own strategies like categorizing the data collected from semi-structure interview based on their purpose.

Yin (2017) strongly advised that to analyze qualitative data playing with the collected data (read again and again) has an immense advantage to come up with a nice conclusion. This study goes through an iterative way and builds some explanations and considers the data collected from literature review with its proposed solution to analyze the interview and document analyzed data.

This is an implication that as it is applied both pattern matching and explanation building techniques of data analysis from the five techniques of data analysis (Pattern Matching, Explanation Building, Time-Series Analysis, Logic Models and Cross-Case Synthesis) stated by (Yin, 2017) p.223-246. Lastly researcher performed the Qualitative Data Analyzer (QDA) Miner Lite data analyzer software installation, data importing to QDA Miner Lite, data coding, themes searching and themes revising. Processes applied in data analyzes are presented here in the below figure.

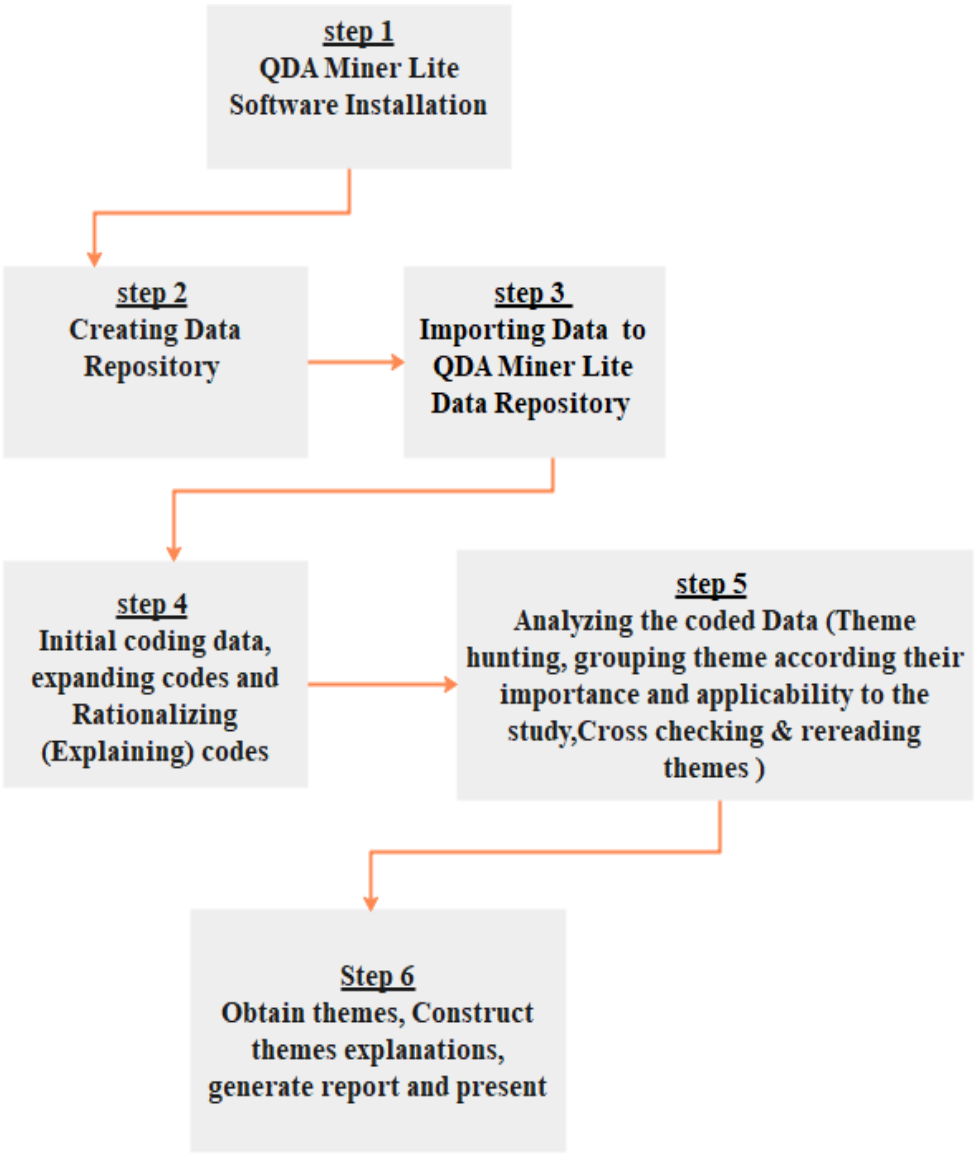

Figure 14: Illustrates steps of data analysis employed on this case study research

3.6. RESEARCH QUALITY ASSURANCE

Research quality can be checked by four test mechanisms. Those four test types are construct validity, internal validity, external validity and reliability. **Construct Validity:** In case study this can be achieved by having multiple sources of evidence and key informants review draft in case study report at the time of data gathering and data arrangement. **Internal validity:** Can be addressed in data analysis by doing pattern matching, building explanations, addressing challenging explanations, and using logic models. **External validity:** Single and multiple case studies can use theory and replication logic respectively in the research design step. **Reliability:** can be obtained

by using case study protocol, develop case study data base (DB) and maintain a chain of evidence at the time of different data collection steps (Yin, 2017).

As (Korstjens & Moser, 2018) cited Lincoln and Guba, trustworthiness in qualitative research fails under the criteria of credibility, transferability, dependability, and confirmability. This research has tried to assure reliability and validity by addressing the required things discussed in the below table. The activities done from no1-7 were all concerned to certify reliability and activities done from 8-14 were concerned to certify validity.

No	Activities done	purpose
1	Performing review of all interview transcripts with contributor at the end of each interview transcription	To permit contributor provide critical evaluation and to confirm accuracy, genuineness and fullness (completeness)
2	Utilizing member checking	To certify dependability
3	Performing transcript review	To ensure reliability (accurate illustrations of participants' words) and provide chance if participant needs to add any more points
4	Collecting data from multiple sources (document analysis and semi-structured interview)	To crosscheck reliability of gathered data
5	Openly telling the role of researcher on the interview to contributor	To build confidence of respondent
6	Telling participants that their consistency is very crucial to the study	To approve respondents input is critical
7	Triangulating contributors' comments with ideas of other sources on the same matter	To assess (evaluate) the accuracy of the respondents' speech

8	Presenting complete explanation of data collection and data analysis processes	To address transferability (generalizability to other contexts)
9	Applying systematic examinations of data gathered from participants	To assure strong research validity
10	Crosschecking appropriateness and richness of data	To certify valid and saturated availability of data
11	Performing interview sessions with enough number of respondents till the level of data collection reached at data saturation and beyond	To confirm data is collected adequately & highly quality
12	Performing open and just free and truth self-reflection to participant with full guarantee for any pre-known risks upon his/her participation on the study	To assure reflexivity for the purpose of free buying knowledge and experience of respondents and to maintain better researcher and respondent relation ship
13	Performing member checking by respondents validating the exactness of their responses on the study result	To assure credibility/ validity
14	Operationalizing checking and re-checking data and proper documentation of the process	To approve confirmability

Table 5: Detail research activities done to maintain quality in the study

In addition to this the researcher performed other very essential tasks to assure the quality of this research by inviting internal experts for framework examination. From the preliminary investigations and crossed data collection, it was understood that ethio telecom has not any DR framework either locally practicable or internationally accepted standard. However, there is an ad hoc recovery and incident management practice in the company. The data collected and analyzed from two divisions of departments and

sections showed that all departments absolutely needs a suitable framework in order to construct their ITDR policies and procedures.

The development of this simplified ITDRPF proposed in this research study for ethio telecom was keeping ideas regarding to the delivery of telecom service in Ethiopia. The proposed framework was shined over the company as it was scored very good result at the time of internal expert evaluation. It opened the gate to bring change on the existing view, practice and patterns of ITDRP in the company believing it will provide support to top level management on the procedural developments of ITDRP for the company.

Experts from Information Systems and Information Security divisions of different departments and sections were participated on the evaluation of the proposed framework for its validity & reliability and also invited corporate systems managers and experts were participated to test the acceptance level of the framework. All the business and corporate systems managers and experts were from the critical functioning areas of ethio telecom different systems. Basically the evaluators were from the mission critical 1, mission critical 2 and business critical functioning areas which the areas were directly concerned areas to evaluate any ITDRP policy, process, procedure and strategy setup.

As the company was obviously showed that it was in need of ITDRPF realization for better data services and IT infrastructure, the result of the evaluation for framework acceptance twinkled high. Thus based on the feedbacks of the experts, the framework was found that a major step forward in ITDRPF services for telecom industry in Ethiopia.

3.7. CHAPTER SUMMARY

In chapter three the researcher explained the research design and methodology applied. Starting from introducing what methodology and methods it passed to a deep visualizations of the methods applied and must be applied so. All the necessary professional processes applied in qualitative case study researches applied in different scholarly works as a methodology were also seen in this research methodology portion.

Hence this chapter carefully showed every movements of the study to reach at data saturation, organization and analysis so that to draw conclusions about the stated research topic in the case company. This chapter supported the study by making a blueprint in the proposal and developed the proposed plans to actions so then to find ways to capture perceptions and attained to an effective approach that have the deepest and richest information. Through the realized investigations on the notion of case-study research design selected qualitative research approach the chapter completed all the tasks of presenting the definitions of terms, the research approach, the research design, defining the unit of analysis and unit of observation, applied techniques for appropriate participant sampling, data collection, data organization and data analysis processes.

The point of reliability and validity was presented with what had been done to approve them in detailed including reasons of tests for validity and reliability. In order to organize data and realized thematic analysis a software called Qualitative Data Analysis (QDA) Miner Lite was used. In addition to this the end to end citation and referencing was done by the supportive application called Mendeley Desktop Version: 1.19.5. All the tools applied in this study were presented at the appendix part of this research paper with their functions. Finally, this chapter concludes by stating scholarly accepted research ethics and witnessed that this research study applied the ethical considerations by presenting different evidences. Results of the processes are delivered in following chapter (chapter 4).

CHAPTER FOUR

4. CASE-STUDY ANALYSIS, FINDINGS, DISCUSSION AND SUMMARY OF RESULTS

4.1. CHAPTER INTRODUCTION

This chapter presents case study analysis, findings and interpretation of the entire research. This study investigates the degree of ITDRPF practices in the selected case company (ethio telecom). As it is already presented in chapter three methodology part, this study employed the qualitative single case study approach by selecting participants purposively. So to present the results of the participants' information the researcher was depended up on thematic meaning extraction from among ideas of respondents invited from two divisions of 5 different departments.

Data collected through semi-structure interview took different lengths were given codes to participants for data analysis and secure anonymity of response.

Lists of Interviewee	Given Code	Locations	SSI length
Director 1	Respondent 1	IT Service Design	55 minutes
Director 2	Respondent 2	IT Service Transition	90 minutes
Director 3	Respondent 3	IT Service Operation	90 minutes
Director 4	Respondent 4	Risk & BC	55 minutes
Manager 1	Respondent 5	IT Service Strategy	45 minutes
Manager 2	Respondent 6	IT Service Design	55 minutes
Manager 3	Respondent 7	IT Service Transition	30 minutes
Manager 4	Respondent 8	IT Service Operation	45 minutes
Manager 5	Respondent 9	IT Service Operation	55 minutes
Manager 6	Respondent 10	Risk & BC	45 minutes
Expert 1	Respondent 11	IT Service Strategy	55 minutes
Expert 2	Respondent 12	IT Service Design	30 minutes
Expert 3	Respondent 13	IT Service Transition	55 minutes
Expert 4	Respondent 14	IT Service Operation	45 minutes
Expert 5	Respondent 15	IT Service Operation	40 minutes
Expert 6	Respondent 16	Risk & BC	45 minutes

Supervisor 1	Respondent 17	IT Service Operation	45 minutes
Supervisor 2	Respondent 18	IT Service Operation	40 minutes
Supervisor 3	Respondent 19	IT Service Operation	45 minutes
Supervisor 4	Respondent 20	IT Service Operation	55 minutes
Specialist 1	Respondent 21	IT Service Strategy	30 minutes
Specialist 2	Respondent 22	IT Service Design	90 minutes
Specialist 3	Respondent 23	IT Service Transition	45 minutes
Specialist 4	Respondent 24	IT Service Operation	55 minutes
Specialist 5	Respondent 25	Risk & BC	45 minutes

Table 6: Interviewee detailed information

The code provided to participants were "respondent and number" and in the analysis part the word respondent is abbreviated as "**Resp"** to refer ideas of respondents. The sessions of semi-structured interviews were held in five categories (face to face held 90 minutes, face to face held 55 minutes, face to face held 45 minutes, over phone call held 40 minutes & over phone call held 30 minutes).

	Face-to-Face			**Over Phone**	
	90minutes	55minutes	45minutes	40minutes	30minutes
	3	8	9	2	3
Total	**20**			**5**	
Grand Total	**25**				

Table 7: Modality of semi-structure interviews and their durations

4.2. CASE STUDY ANALYSIS

In this section the researcher provides the detailed analysis and description of the case studied completed by semi-structure interviews and document analysis. Case study analysis of this paper was followed by mapping the research questions and specific objectives sated at chapter one of (1.4 and 1.5.2) respectively of this study. The ups and downs in this study was aimed to achieve a considerable response to the research questions so that to realize the specific objectives seated in chapter one (1.5.2). The

research questions and objective were mapped (see below table) and interview questions was created based on the two premises.

No	Research Questions	Specific Objectives
1	What could ethio telecom be benefitted from attaining ITDR?	To figure out the importance of having ITDR.
2	Why ethio telecom doesn't have ITDR?	To investigate the challenges to attain an ITDRF in the company.
3	How ethio telecom can attain a feasible ITDR?	To study the means to have an ITDRF.
4	Where ethio telecom can launch its possible ITDR?	To Propose an ITDRF based on the research findings for ethio telecom.

Table 8: Mapping of research questions and specific objectives

4.3. ITDR GAP INVESTIGATION

Developing a DRP is not an easy and one time task, it requires different complicated activates and processes (Hawkins et al., 2000). According to the research contributors' feedback ethio telecom had tried to launch an ITDRP in 2015 without studying critical functioning areas of the organization and without project feasibility study and plan. The major reasons that was presented by respondents were, ethio telecom was vender dependent company and still it is vendor dependent and internal staff members even with high expertise level experiences and knowledge were not invited to participate in the major technological feasibility study, even most of the top management members did not need to realize the ITDR, the business department of ethio telecom was neglected to provide their inputs for the project, there was/is no road map which supports as a frame of references in the company, things presented by vendors was accepted without cost and benefit analysis.

These issues created gap on deciding where to place the DR site, what important ITDRP components should to behave, what will be the DR implementation strategy, how the DR operations will be performed. During the interview time respondents explained their feelings that ethio telecom should work more on follow up awareness creation and

team synergy to attain ITDRP. Those all alarming gaps were considered in this thesis. The evidences given by respondents were presented here in the below paragraphs.
*"In ethio telecom many solutions are purchased without feasibility study and continuity benefit from the solution. Let if take the start to realize DR in 2015, vendor persuaded to some member of managements to have ITDRP we some of us were not invited to contribute our ideas and experiences. Then after some time the company call to only IT departments to communicate about assignment of staff and to decide the place where the DR should be housed. Finally, we did not agree on the place because it was proposed wrong place, but some groups agreed and signed and then with no selection of systems the hardware installation was done for all Information systems 'Systems'. After a year all the servers, enclosures, storages were removed and installed to main site for system expansion. You see the gap it was at the first stage to be decided which of the systems need to have ITDR and the like unless simply need without knowledge could not attain the objective of ITDR." [*Resp *7, 11, 14]*.

"Lack of Management follow up, concerns, responsibilities, politics, lack of strong control & follow-up, zero emphasis to the DR solution, very poor attention to the value of data, less attention to threats and zero market computations. Generally, the human element of the company is knowingly and unknowingly not matured for such kind of solution." [Resp – 10, 12, 15, 17].

When respondents were asked if they face any major outage they responded as follows. *"Yes, the most once are disc crash, commercial power created burning hardware, disc failure many times system outage like ERP, failure of email systems for consecutive three years 2018, 2019 and 2020 due to virus attack, customer Care and Billing (CCB) server air conditioner failure CBS failure due to technical problem and flood, untrained human created data loss." [Resp – 1, 2, 7, 8, 11, 13, 19, 22]."*

The question presented to respondents 'How do you explain your knowledge towards ITDR?' to get their level of understanding about ITDR was summarized as follows. *"It is securing data and infrastructures and providing services without any interruption. DR is a solution to protect data and go on services before and after some incidents. DR*

is making data accessible for business processes by securing hardware and software and Network connectivity." [Resp – 5,9,13,18].

The points raised by the respondents in this thesis showed that the investigation on the issue is highly required. The study extracts out the facts and causes why ITDRF is a critical issue in ethio telecom context. Furtherly the study investigated that management of ethio telecom specific to the CEO before 2018 assumed implementing ITDR is to fulfill the organization's corporative requirement for sample not to solve critical problems. As respondents explained the advantage of having ITDR is an endless guaranty of data, hardware and software resources of the company.

In addition of top management lack serious follow up and assigning task force to perform their daily tasks, ethio telecom lacked customized & feasible ITDR road map and it did not invite the internal experts and mangers to discuss the possibility of ITDR before project start. Therefore, successful ITDRF has been a considerable option in seeking critical data, service and infrastructure safety. There was a maintainable agreement among the participants that ITDR is not an optional it is a must to have and it provides really an advantageous business performance in different security terms.

4.4. AWARENESS OF IMPLENENTING ITDR IN ETHIO TELECOM

Even a single member of ITDR taskforce must believe what the importance of ITDR: Though it is challenging to make all member of ITDR have positive ideas about launching ITDR. There are different gaps visualized by respondents of this study and the aim of this qualitative case study is to show and propose the means to solve the gaps (issues) on developing ITDR. The Points listed out in 4.3 above gives a typically good thoughts and highly benefiting experiences sharing and notes to ethio telecom for how, why, where should it implement the ITDR. As respondents presented their evidence the company has no financial capital problem. Rather it still did not internalize the advantage of having ITDR over fulfilling the corporate requirements.

4.5. CHALLENGES TO ATTAIN ITDRF IN ETHIO TELECOM

Respondents explained that there are different blockages which hinders to realize ITDR in ehtio telecom. The summary of respondents to this matrix was laid at poor company culture and attitude towards having ITDR.

"The biggest challenges are readiness gap, lack of focus, politics, skill and knowledge gap. You are investigating an advanced solution beyond our current knowledge as a company because we started even the concept of data center may be few years back and yet we don't have improved and standardized data center. Even if we don't have standardized data center DR is mandatory as it is a replica of the commercial processing systems." [Resp -4,12,20, &25]. Respondent 5, 8, 13, 16 &24 also said *"no department put in its future plan to accomplished, commitment problem, poor RA and BIA, lack of finding benchmark frameworks, poor alertness for critical systems down times, Poor knowledge of data protection."*

The questions: How communications go in your company aimed to service restoration from any outages? And: Does your division/department perform RA? If yes could you, please explain in detail? Were responded as follows respectively. *"Since there is no dedicated team member every time you noticed incident you will rush not to find a solution, but to find a solution provider either specialist, expert, analyst who ever with the specific assignment." [Resp – 15, 17, 18, 20, 21, 22, 23]*. *"Yes, sometimes two times per year sometimes once per a year, but it is common minimum of once per a year, but it is with no lesson taking. So if you could not learn from it and go to solve based on that it is meaningless, so it is not that much improved." [Resp – 1, 2, 3, 4]*.

Respondents raised very important points about the existing challenges in the case company ethio telecom which they could hinder the attainment of ITDRP. The major points raised were absences of responsible management, lack of follow up in every functioning area, less attention to DR and absence of customized road map for ITDRP which is suitable to the company ethio telecom. All participants were agreed there is no financial problem in the company.

4.6. LEVEL OF IMPORTANCE HAVING ITDR TO THE COMPANY

Developing ITDR has various steps. Those steps are useful and provides 7 importance such as eliminates confusion and error, minimizes disasters to corporate operational systems, being an alternative during disruption, being safety of company personnel, avoids dependency on some staffs, keeps company data and supports on an orderly recovery (Hawkins et al., 2000). According to the respondents of this study having ITDR can benefit to the company by providing support to protect data and infrastructure resources from disaster. It indicates what measures should it be taken, distinguishes unsafe situations, increases performance of workers, creates better thought of scalability and better customer retention, facilitate and guarantees continuity of the business, protects assets from loss, minimizes extra costs, prevents customer loss, minimizes unreasonable employees turnover or termination of staff and it helps company to have futurity plan and predictable journey. Compiled evidences were presented here in the below Paragraphs including the questions.

What are the threats to your systems, data and infrastructure resources currently? *"There are many threats to telecom operators by nature because it applies complicated systems and infrastructures with this limit also have varieties of data. However, in case of ethio telecom the most considerable threats are internal fraud, mob, virus attack, flood and fire." [Resp -1,2,3,4,7,11,20,23]*.

What are the main advantages that ITDR can give you to attain and enhance BC in your Company? *"DR realizes operational systems restored to their normal functioning and data becomes safe for any business transaction. So as DR is a one single part technical element of BC it helps making the services continue and restored to their normal situations. If ethio got DR practically, at minimum it could minimize financial loss, it gains customer satisfaction, it attains good status, and it can restore any incident with in shortest time." [Resp - 10, 11, 15, 17,19]*.

Could you please explain me how ITDR can assist your organization in protecting data and IT services? *"The point is if there should a DR it must be reliable DR not for formality and the like. So now if ethio have DR unquestionably it is default who is*

responsible for what action and goes smoothly, every activity will be synchronized either real-time or in some fractions of seconds or hours. Having reliable DR creates greater confidence on the company and it brought higher reputations and an immense data and infrastructure safety." [Resp - 1, 5,6,7,8,9,10,16].

Do you consider having ITDR as time and resource consuming process? *"Totally no. because we do no one time what will happen, either separately to our DC or through the whole town Addis Ababa. So DR is a concept of making ready for safety for specially data and services and infrastructure. So if something happens you gain if not happen still you gain because a s a technology business company you create confidence and you create employee safety to do their work in an owner ship sense of synergy." [Resp - 2,3,6,7,10,13,14,16,20,23,24,25]*.

Could you please explain me the importance of ITDR framework for ethio telecom? *"Having ITDR does not mean completely making the organization free of any risk, but it reduces the risk and it supports you on minimizing the risks. So having ITDR framework supports by visualizing and leading how to attain a workable and exercisable IDR on making the action plans, before, during and after some events of disasters. ITDR is aimed to react technical related disastrous events, and to do so there must be frame of action how to do, by whom, with what resources, in what speed of time and with what level of acceptable loss of data. This all are compiled in a single frame. So framework helps as leading and directing compass to exercise the ITDR. It is something a leading map." [Resp- 1,4,5,10,11,16,17,20,21,25]*.

If some disaster happens, just like flood, fire or mob around and within this Addis Ababa city what is at your company hand to defend such situation? *"The solution would be only reconstructing from scratch." [Resp 1,2,3,4,5,6,7,8,9,10,11,12, 13,14,15,16,17,18]*.

Could you explain me the emphasis of having ITDR on ethio telecom IT staffs? *"Positive impact. You see if there is reliable ITDR there will be a real exercise in end to end all different ITDR tasks such as trainings, mock disasters, maintenance and updates, RA, testing for ITDR, conducting off-site backups and other preventive actions; on doing such exercises the IT staff will become highly knowledgeable. And*

there will not be ad-hoc team construction finding someone who would be responsible to solve for some disasters here and there." [Resp - 3,4,8,9,10,14,15,16,17,18,19,20, 24,25].

4.7. IMPLEMENTATION STRATEGIES OF ITDR IN ETHIO TELECOM

There must be a consideration of ITDR in all steps of System Development Life Cycle (SDLC) which means in all the procedures of Strategy planning, System Analysis, Feasibility Study, System Design, Implementation, and Maintenance (Aggelinos & Katsikas, 2009). An organization wishing to have ITDR should include the eight ingredients of CIO and DR experts' advice which are: inventory hardware and software, define RPO&RTO, lay out who is responsible for what & identify backup personnel, create a communication plan, let employees know where to go in case of emergency, make sure your SLA include disasters/emergencies, include how to handle sensitive information and test your plan regularly (Schiff, 2016).

In case of ethio telecom the respondents raised that the implementation strategy should start from identification of possible disaster scenarios. After that there must be a high consideration to top management follow up, building permanent DR team, DR plan documentation and location selection such as (distant from all the primary systems, far from congested commercial power wiring, far from air craft station, far from main roads and historically free of earth quack and volcanic eruptions). The respondents added that the set up should be mirrored type ITDR (Active=>Active or Active=>standby data replication at both sites with shorter period of time) and similar hardware and software installations. Below are the compiled evidences of respondents including the interview questions.

Could you please explain which systems should be prioritizing while deploying an ITDRP? *"When deploying ITDRP it should be very selective. So in case of ethio telecom our systems are already grouped as mission critical, business critical and corporate systems. The mission critical systems are grouped into two mission critical one and mission critical 2. ITDRP for ethio telecom should be focused for only the mission critical systems (Tier 1). The systems in mission critical one (tier 1) are CBS,*

HLR/HSS and CRM; the systems in mission critical two (tier 2) are IPCC, SMSC, SDP, Bulk SMS, USSD, E Top UP, ERP, ISP, UNMS, OSS, RMS, TT, and FMS. Business critical systems are SOC, FMS, UAC, Email Exchange, EIR, E-CAF, VSS & IDAC, NMS, EMS, ITSM, RA, Firewall, USM, VMS, MMS, WAPGW, CRBT, Anti Spamming, and RWM." [Resp – 1,2,3,4,5,6, 7,8,9,10,11,12,13,14,15,16].

Could you please explain me how difficult is for IT staff to respond to their normal duties and follow up ITDRP activates? *"That is very challenging. Because while you are assigned to do normal task suddenly if there is some incident your forced to handle it: when you go in different tasks with in one day sometimes you become unsuccessful in all tasks, why because you are not ready for the incident, you don't have tools starting from accounts to solve them, even you don't have gate pass to inter to different rooms for that you start sending mail for approval, then accounts another process so your day becomes end without handling anything."[Resp-17,18,19,20,21,22,23,24,25].*

How do you manage the service interruption specifically unplanned down time occurred in your organization currently? *"Basically in ethio there is I 2000 system which the monitoring section always monitors the different alarms like Critical, major and minor alarms. If those alarms level at critical are unable to solve with in some seconds or minutes there will be incident. To solve suddenly happening incidents there are many ups and downs in our company because you do no to whom the case it should be sent. For formality we do have standby team from different sections but since incidents are unplanned most of the assigned teams are not available when something happens and even if they are available they are not the exact person to fix the issue. Many times ethio is paying too much dollars for maintenance support to vendor. The reason is because we don't have separately assigned team for any incidents and it seems ethio did not include the operational incident supports included in its SLA. Sometimes even to plug a cable you need approval because you are not a concerned team [Resp-11,12,13,14,15,16,17,18,19,20,21,22,23,24,25].*

Could you please explain me how the implementation of ITDRP should be in your organization? *"The implementation of ITDRP in ethio should be focused on Mission critical Systems that directly impact customers when they disrupt and demands 100% availability all the time to provide the services of the company. Tier one Mission Critical*

*systems: - systems where the company depends on to provide basic mobile service. The impact of the disruption to these systems in terms of revenue, national communication issues is huge and could create public outrage. The primary system needs to have****: - DR sites + Local Redundancy + Backup which is real time (or near real time) data*** *update (synchronization) at both sites.*

Local Redundancy is necessary why because during Disaster: - Using DR site is not a quick solution as it has its own delay defined by RTO and transmission/link stability issues. DR is more applicable when Disaster happen due to irreversible factors like fire, war, earthquake or when it is impossible to recover within the RTO. So the Local Redundancy should be designed with load sharing to avoid single point risk and to gain advantage of capacity. The ITDRP should be placed somewhere in Ethiopia owned by ethio telecom with necessary vendor support. When we come to Tier Two Mission Critical systems: those are systems which provides service to many customers and whose failure directly affects customers, revenue and image. The primary system needs to have: - ***Local redundancy site with load share + Backup. No need of DR.*** *But, local redundancy and backup should be fully utilized. For Business critical systems: All business support applications and used for internal operational efficiency that need availability near to but not necessarily 100%. This needs* ***at least server based redundancy + Backup and Local redundancy shall be applied based on BIA finding****. Its dependency and disruption impact will be taken in to account" [Resp-2,3,5,8,10,14,16,17,19,22,23,25].*

Could you please explain me the practices of handling service interruptions, ways of communications during incidents and learning notes? *"There is a practice of assigning standby staff members communicated by email to all functioning areas. Those activities of assigning standby team, communicating weekly emails to different functioning areas all this are some good starting, but it is not that much improved way. For example, someone assigned to provide support in a given system with no privilege is not good. The assignment by itself we can good practice and easy to whom to communicate; however, the person becomes none expert to that area at this time we can say very poor communications to target fully handling concerned one. So in ethio in every meeting we raise about that like incident resolution mechanisms must be documented and should be used for the next similar cases, however with no clear link*

blockage the action is an action of meeting only no exercises on the ground. Performed eghgh detail incident analysis is done by vendor as called root cause analysis; even that analysis we do no the reality from what perspective they are analyzing. Ethio simply punishes the vendor based on the SLA and Operational Level Agreement. In general, we do have very poor incident handling mechanisms, ways of communication, and taking incidents as learning experiences. Even for root cause analysis we are vendor dependent. Vendor also provides the analysis possibly as sweetest as lowest punishing analysis we know but we accept them; even ethio is not getting enough from SLA and OLA penalties from vendor" [Resp 1,2,3,4, 9, 10, 11,12,13,14,15,16, 25].

What elements do you think to include in your ITDRP makes successful? *"To implement reliable and successful ITDRP it needs employments of time, technology, people, infrastructure, finance, process, ITDRP documents, continuity management approval (to fix either the DR should be rental or owned by company), process, staffs to be assigned permanently on ITDRP tasks, the necessary technologies and management follow-up." [Resp 1,2,3,4,7,8,9,10,11,12,13,14,15,16, 18,19,20,21,25].*

4.8. REVISING THE FRAMEWORK

The problems of not having an ITDRP were said by respondents that lack of responsibility, lack of top management follow up, implementation problems, poor resources mobilization, ideological and political issues in the company, lack of readiness to adapt ITDRP, knowledge & skill gap, lack of focus to include ITDRP in operational activities, poor risk analysis and visualization, ignorance of ITDRP to include in every functioning areas and lack of commitment from staff to management. The analysis result showed there is no top management approval problem and there is no facility and finance problem in the company. So ethio telecom should have mirror site with active =>Active setup with Secondary site that mirrors the primary site which it must be managed and owned by ethio telecom. The systems to have ITDRP must be for only tier one mission critical systems with additional local redundancy and backup.

The proposed ITDRP framework for ethio telecom was based on the preliminary study and detail literature reviews, however after data collection and analysis the findings showed that the proposed framework needs additional points in to it and deletion of

some points from it. So modification and revising to the proposed framework becomes mandatory. After modification the findings of investigations would be included. The modification was done by including the phases of developing ITDRP as a supporting to the solution and the issue of management follow up is included in the frame for overall follow up of the ITDR; the below figure illustrates this all.

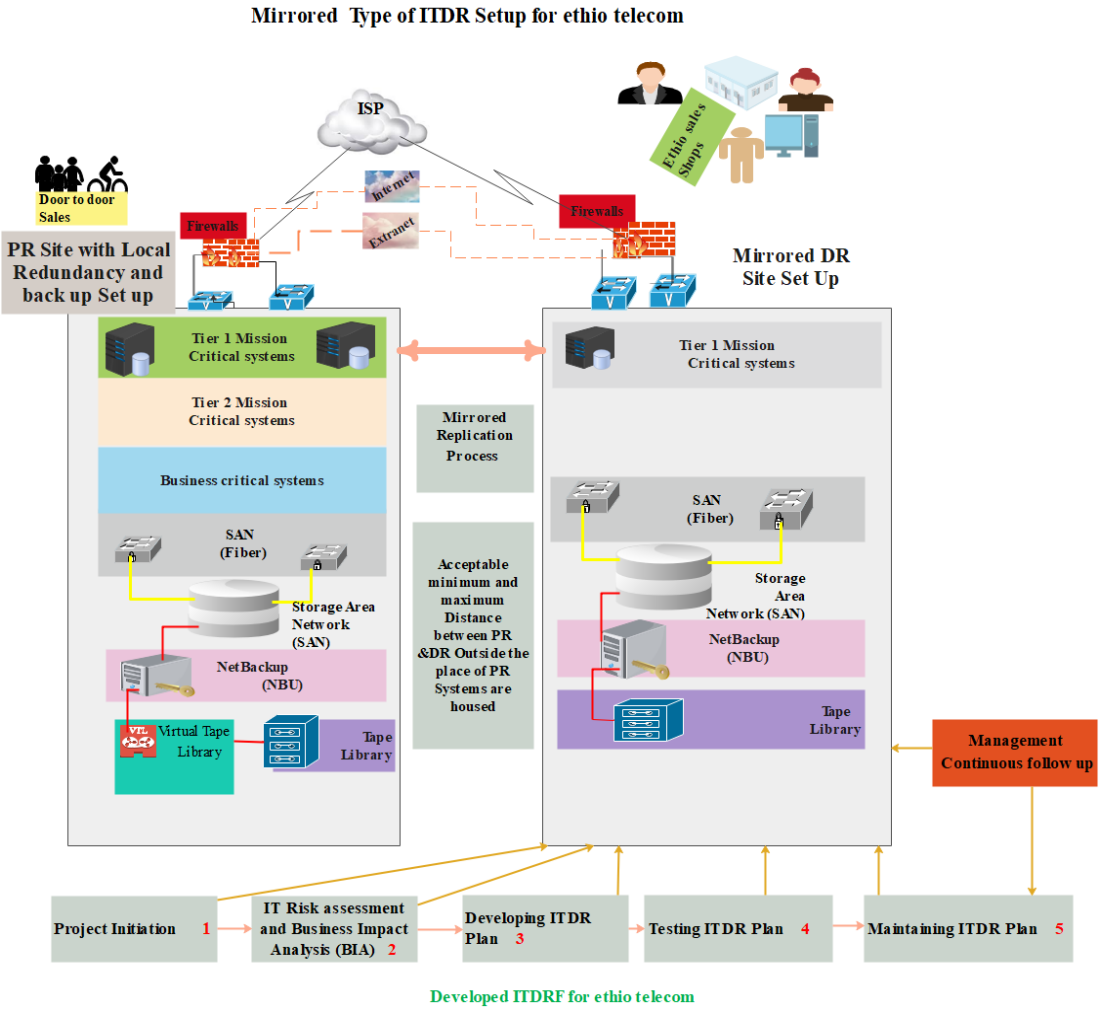

Figure 15: The Modified and final developed ITDRF for ethio telecom

4.9. TESTING THE FRAMEWORK

The developed framework was given to internal experts for reliability test and validity checkup. The testing aspects were mapped in to 2 domains and 20 sub domains. The first domain was Research Methodology & Data Analysis totally weighted 30% and has 6 sub domains each weighted 5%. The second domain was appropriateness and achievability of the developed ITDR Framework for ethio telecom which weights 70% and has 14 sub domains each weighted

5%. There were 10 internal experts selected to validate the developed framework. The evaluators were given a name "Evaluators" followed by sequential numbers (meaning Evaluator 1, Evaluator 2 … up to 10) to make easiest result data presentation provided by the evaluators. The details of the procedures performed was presented in Appendix _C.

4.10. DISCUSSION

Data and infrastructure of telecommunications should be properly managed and protected. Ad hock disaster recovery mechanism can bring a huge amount of data and infrastructure loss to IT and telecom companies. To minimize such losses a company in charge of technology should implement different data recovery mechanisms. The best one is preparing separate disaster recovery site. Since data is a vital asset of a company it needs greater attention. To address maximum high availability and data secured implementing mirrored replication of main site and DR site of mission critical systems is recommendable. The purpose of the study was to develop an ITDR framework for ethio-telecom. In this regard the points that the current practice of ITDR, ITDR gap investigation, the challenges to attain ITDR, awareness of implementing ITDR for mission critical and business critical systems was addressed.

The interview data shows that there is enough awareness regarding to IT disaster and its impact. However, currently there is no ITDR in the company. Instead there is ad-hoc incident management for services restoration and resolve any service interruptions. This shows the selected divisions has knowledge of the severity of ITDR which could threaten their mission critical and business critical systems. To the opposite of that, if the systems face kind of disaster, the company goes ups and downs to overcome the risk. Respondents of the research has raised that the company has no resource problem. The main bottleneck is lack of incorporating ITDR tasks in a strategic plan of each and every concerned division and departments. At this time technology companies are challenged by cyber security threats; this world wide threat also is a high concern and exposure of etio telecom. The logic is that the company lacks feasible ITDR.

Some interviewees argue against having ITDR because the company lack standardized DC. Most of the interviewees agreed to have separate ITDR even if having less standard DC. Most of the respondents' intension was the company can own highly secured data and un interrupted service delivery plat forms if it must work focusing on the data

securing technology options such as implementing and exercising ITDR. Ethio should not work on problem solving after IT disaster is happened. It must be prior than of any IT disasters so that it would highly minimize or totally eliminate many hazards. The participants hate the current ad-hoc way of ITDR means being lacked dedicated DR team members. This theseis agrees was the point *"People are responsible for designing, implementing, and monitoring processes intended to safeguard data. However, people make mistakes every single day"* (Snedaker, 2007). The revolving ITDR threats in ethio telecom can be minimized by the cooperation of the people inside the company.

Since this thesis has used the freely available resources, the researcher believed that this lack of enough relevant materials has negative influence on the result of the investigation. In addition to this all the points raised under limitation has their own impact to this thesis.

4.11. CHAPTER SUMMARY

In chapter four this thesis presented the case study analysis and findings. A standard confirmation of successful ITDRPF would be concrete when the gaps investigated becomes improved. In that respect this chapter recognized the view that support to improve the ITDRPF gap in ethio telecom. This chapter discovered and approved that developing ITDRPF was a vital way of increasing organizational data, service and infrastructure safety. This concept has already verified in detail convoying with the data collection based on the SSI from the respondents.

This chapter also clarified the best ways of sensing ITDRPF gaps via the model developed by the researcher. The solution to solve the endless problems in the organization knocking the head of two divisions because of they lack to implement the solution has been explained in detailed through the adapted framework. The findings showed that ITDRPF is highly needed in ethio telecom. Finally, this chapter presents a modified and final ITDRPF for ethio telecom with supporting phases of developing ITDRP.

CHAPTER FIVE

5. SUMMARY OF RESULT, CONCLUSIONS, RECOMMENDATIONS AND FUTURE RESEARCHES

5.1. CHAPTER INTRODUCTION

This chapter presents the discussion, conclusion and recommendation based on the stated objectives of the study. The four objectives of the study were to figure out the importance of having ITDR, to investigate the challenges to attain an ITDRF in the company, to study the means to have an ITDRF and to propose an ITDRF for ethio telecom that can be applied to implement ITDR process in the case company ethio telecom.

Four areas were investigating which those: - ITDR gap, challenges to attain ITDR, level of ITDR necessity in the company and way and strategies to realize ITDR. A semi-structured interview and document analysis was used as primary and secondary data collection tools from the Information Systems and Information Security Divisions of different departments and section by involving 25 respondents. Finally, data was analyzed by QDA Miner Lite and findings were presented; based on the research findings an ITDRF was developed for ethio telecom by adapting from (Uddin et al., 2015). The developed framework was provided to internal experts for validity and reliability and acceptance test. The score shows 88.12% achievable and acceptable framework for ethio telecom.

5.2. SUMMARY OF RESULT

In the context of ethio telecom the study found that the solution of ITDRPF is not an optional, rather it is a critical mandatory. The study employed the qualitative research case study approach employed 25 research participants. The data collection instrument was employed purposive sampling which it was suitable for case study researches. The result showed that in ethio telecom there is no financial or resources scarcity to attain ITDRP, but the issue which is hindering ethio from having improved ITDRP is the human element from lower staff to top management lacked follow up and continuous evaluations. The skill and knowledge gaps in ethio telecom member staff were stably agreed they could be solved by trainings.

Systems were classified in to miss critical 1, mission critical 2 and business critical. The participants of the thesis visualized that ethio telecom is interested to have ITDRP for only mission critical 1 systems and others are proposed to have local redundancy and back up. In the data analysis for the question why ethio telecom still does not have ITDRP was responded in summary lack of cooperative and synergy among staff, lower management, middle management and higher management to have ITDRP and the internal politics. All the respondents shared their ideas that ITDRP is critical for ethio telecom.

The developed ITDRPF for ethio telecom was aimed at filling the gaps of the company by analyzing the data collected from the respondents of 2 divisions of 5 different departments of purposefully selected sections. The framework includes the phases of developing ITDRP, selecting appropriate and available technology, set up secondary DR Site and design of facility. The ITDRP for ethio telecom is confirmed by respondents active—active set up with ethio telecom owned DR site and must be housed in a comfortable area which is free of known natural disasters, considerably far from main site, it must have separated teams working as other operations and top managements must give high attention. The analysis shows that if something catastrophic happens in Addis Ababa ethio telecom does not have any at for survival.

The proposed framework was given to 10 internal evaluators to evaluate in 2 domains called Research Methodology & Data Analysis and Appropriateness and achievability of the Developed ITDR Framework for ethio telecom. Those 2 domains have 20 sub domains 6&14 respectively in each weighted 5% and the sum of the points from each domain is up to 100%. The evaluation result was analyzed using Microsoft excel by manually inserting the provided evaluation result point for each sub domain and the score showed that 88.12% of the framework is valid and reliable and can fill the existing gap in ethio telecom.

5.3. CONCLUSION

In conclusion, there are a few sector companies which they exercise ITDR assured from the freely gained society of web resources talking about ITDR. However, there was no any document which was written specific to ITDR in telecom. The freely existed

resources talking about ITDR and ITDRP was done in banks, smart cities and counties. This thesis was done for telecom ITDRF by applying a detailed literature review. The review was included documents of journal articles, books, unpublished materials, company processes and procedure which all raised ideas relevant to ITDRF in different IT sectors.

This investigation concluded that ethio telecom has no resources problem and management approval problem to accomplish ITDR. Similarly, there is no problem of budget and resources allocation; the investigated problem is implementation problem. This study concluded that there is very poor risk analysis and BIA which leads to advanced solutions for disasters like natural and manmade. The company is providing different types of telecom services by owning many different systems, however the guarantee of all systems from different catastrophe is under question. Respondents had knowledge of different frameworks like ITIL and COBIT, but they confirmed that those frameworks are bulky and they need detail customization which suits to ethio telecom which still does not done in the company.

This qualitative research case study approach fully responded to the research questions so as to attain the research objectives and come up with modified and customized ITDRF for ethio telecom. This framework is developed to solve the existing gaps in telecom sector specific to ethio telecom. Other researchers' or attracted groups can use this thesis as a reference in developing ITDRF by incorporating some modifications depending on the size and need of research conducting sector. This study has visualized a lot of gaps in chapter 4 gap analysis part which they need quicker solutions. Finally, the research finding shows that, the need of ITDRF for the company is high.

5.4. LIMITATIONS OF THE STUDY

Research limitations are weaknesses of a given study which all are beyond the researcher's capacity to come up with success over them from their constraining (Theofanidis & Fountouki, 2018). Even though this study provides very useful learnings considering to DR activities, there are minor limitations that has to be said here and can be used as a feedback for future research. Hence this thesis work consists the following two constraints over its valuable contributions.

The study is limited to the available and accessible materials towards the literature review and data collection from the selected case company ethio telecom. In the data collection due to fear of Corona Virus Disease 2019 (COVID – 19) some respondents were not harmony to give their interviewee face to face even by treating the COVID-19 rules. For this reason, conducting interviews over the phone with some plangent communications was an option not to push participant's right and consent.

The findings may not be generalizable to other organizations because of the concept of ITDR and its framework differs from company to company. The interview of 4 directors, 6 managers, 6 experts, 4 supervisors and 5 specialists in total 25 participants in the selected company provided an opportunity to gain an in-depth understanding of the issues related to DR gap particularly in the selected company ethio telecom. However, more case studies would be needed to conduct in other organizations so as to determine whether the experiences of this particular organization can be replicated in other organizations.

5.5. RECOMMENDATIONS

IT dependent companies and telecom providers in general are recommendable to have ITDR. The implementation may vary from company to company and from size to size. Ethio telecom is a huge monopoly telecom company providing all telecom services in the developing country Ethiopia. The company needs to have ITDR as results showed from the analysis, but it lacked a benchmark of ITDRF and there is lack human element coordination to attain ITDR. In the preliminary and main investigations of the study raised some points ethio telecom had tried to launch ITDR before 6 years without detail study of ITDR.

The try was not incorporated IT risk analysis, system categorization, technology setup, criteria to select area, DR documentation, team creation and team capacity development. As the investigation shows that there was also dis agreement among team members regarding to the area selected, the strategy chosen, the set up design, the infrastructure presented for discussion and the operational plans how it would be operated. But the top level management gave a direction for implementation without

the believe of the team for the formality of corporate requirements. However, with no functioning all the hardware was removed and used for different system capacity expansions in the main site after 8 months of launching the ITDR. This shows that when there is no synergy, smooth leadership and work oriented management follow-up even with lot of many and resource company can become poor.

The case already presented helps to recommend that any company needing to have ITDR should first perform detail risk analysis and BIA. And then concerned functioning areas must be communicated clearly and requested for their skill and knowledge support. Some of the problems happened and presented in the statement of the problem of this study shows that the company should have ITDR. So this study recommends to ethio telecom to use the proposed ITDRF for its advantage as a roadmap for attaining ITDR. In addition to the above recommendations it is also recommendable that ethio must minimize vendor dependency by upgrading its own staffs. Finally, the researcher recommends that when ethio needs to start ITDR project all functioning areas must be invited, ethio telecom must open chances to local staffs to show their performances in different projects specially ITDR.

5.6. FUTURE RESEARCH

This case study research investigation was employed in telecom sector; other interested researchers can conduct qualitatively in other sectors with some adaptations. The investigation mechanisms grouped in this study under the SSI question like ITDRgap investigations, Challenges of attaining ITDR, ITDR level of importance and ITDR implementation strategies this four of them also can be studied separately in either qualitatively or quantitatively. Specially the ITDR level of importance is recommended to be studied quantitatively and the other qualitatively.

The developed ITDRF is a more generic an inclusive of all systems in the company any interested scholar can investigate in a more specific manner. This study has slightly highlighted the points of IT risk analysis and back up mechanisms; an interested applicant can investigate advantage of IT RA to strength security aspects of any IT dependent company. Lastly researcher has a recommendation to the coming researchers

to investigate Information Technology Disaster Recovery Plan framework (ITDRPF) in telecom.

5.7. CHAPTER SUMMARY

Points raised in in this chapter were summary of result, conclusions, limitations, recommendations and future researches. This chapter has presented the summarized result of the case study. The conclusions presented precedence by points which were not addressed in this research called limitations. And has put the next research areas.

REFERENCES

Accelerite. (2014). *Disaster Preparedness : Focus on People , Processes and Technologies*. https://www.channelfutures.com/from-the-industry/disaster-preparedness-focus-on-people-processes-and-technologies

Adams, W. C. (2015). Conducting Semi-Structured Interviews. In *Handbook of Practical Program Evaluation: Fourth Edition* (Issue August 2015). https://doi.org/10.1002/9781119171386.ch19

Adedayo, S. (2014, October 30). Disaster Recovery Strategy and Maintenance Plan.

Admin of Open Minds. (2018). *Creating a Disaster Recovery Plan*. https://www.openminds.co.uk/blogs/creating-a-disaster-recovery-plan/

Aggelinos, G., & Katsikas, S. (2009). Integrating Disaster Recovery Plan Activities Into The System Development Life Cycle. *Association for Information Systems AIS Electronic Library (AISeL)*, 76. http://aisel.aisnet.org/mcis2009/76

Akhtar, M. I. (2014). Research design. *Research in Social Science: Interdisciplinary Perspectives*, *September*, 68–84.

Al-qattan, M. B., Buqawa, A., & Mirzal, A. (2017). *A Study on the Disaster Recovery System in the Information Technology Unit of the Ministry of Communication of Kuwait*. *August*.

Alhaidari, F. A., & Atta-Ur-Rahman. (2019). Telecommunication networks in disaster management: A review. In *Journal of Communications*. https://doi.org/10.12720/jcm.14.6.432-447

Baham, C., Calderon, A., & Hirschheim, R. (2017). Applying a layered framework to disaster recovery. *Communications of the Association for Information Systems*, *40*(1), 277–293. https://doi.org/10.17705/1cais.04012

Benjamin, S., Julius, S., Tom, K., Shula, B., & Jackie, W. (2018). *Saturation in qualitative research: exploring its conceptualization and operationalization*. https://doi.org/10.1007/s11135-017-0574-8

Bocian, M. (2009). *Data Center Business Continuance and Disaster Recovery*.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brooks, J. (2019). *How Much Does a Service Outage Really Cost a Telecom Company?* https://www.aerialapplications.com/blog/how-much-does-a-service-outage-really-cost-a-telecom-company

Burns, A. (2015). *Action Research*. *18*(1), 171–196. https://doi.org/10.21608/jfss.2020.106049

C.R.Kothari. (2003). *Research Methodology Methods&Techniques* (Issue 1). https://doi.org/10.16309/j.cnki.issn.1007-1776.2003.03.004

California Judicial. (2017). *California Judicial Branch Disaster Recovery Framework*.

Calik, E., Kaya, H., & Sen, B. (2013). *Disaster Readiness of Hospital Information Systems : A Case Study from a Turkish University Hospital*. *September*.

Chow, W. S. (2000). Success factors for IS disaster recovery planning in Hong Kong. In *Information Management & Computer Security*. https://doi.org/10.1108/09685220010321326

Chow, W. S., & Ha, W. O. (2009). Determinants of the critical success factor of disaster recovery planning for information systems. *Information Management and Computer Security*, *17*(3), 248–275. https://doi.org/10.1108/09685220910978103

Chowdhuri, S. R. (2011). *Oracle ® Fusion Middleware*. *1*(April), 1–18.

Cisco. (2008). Disaster Recovery : Best Practices. *Cisco Public Information*, 1–18.

http://www.citc.gov.sa/English/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/PL-PM-014-E-Guidelines on Disaster Recovery Planning for the ICT Industry.pdf

Dickson Adom, Emad Kamil Hussein, & Joe Adu Agyem. (2018). Theoretical and Conceptual Framework: Mandatory Ingredients of A Quality Research. *International Journal of Scientific Research*, *7*(1), 93–98. https://www.researchgate.net/publication/322204158%0ATHEORETICAL%0A

DiDio, L. (2019). *ITIC 2019 Global Reliability Survey Mid-Year Update*. *508*. https://www.ibm.com/downloads/cas/DV0XZV6R

Dolma, S. (2009). The central role of the unit of analysis concept in research design. *Istanbul University Journal of the School of Business Administration*, *39*(1), 169–174.

DR Test and Maintenance. (2010). Retrieved from http://disasterrecoverypartners.org/?p=448

E.Stake, R. (1995). *The Art of Case Study Research*. Sage Publications, Inc. https://books.google.com.et/books?hl=en&lr=&id=ApGdBx76b9kC&oi=fnd&pg=PA7&dq=robert

Elmusharaf, D. K. (2012). Qualitative Sampling Techniques. *Theory and Practice in LanguageStudies*,*2*(4),784–792. http://www.academypublication.com/issues/past/tpls/vol02/04/20.pdf

European Commission. (2020). *EU science hub - POTEnCIA*. 1–4. https://ec.europa.eu/jrc/en/potencia/jrc-idees

Evolve IP. (2018). *Top Benefits of Information Technology disaster recovery planning (ITDRP)*. https://www.evolveip.net/blog/4-benefits-disaster-recovery-planning

Gerassi, L., Edmond, T., & Nichols, A. (2017). Design strategies from sexual exploitation and sex work studies among women and girls: Methodological considerations in a hidden and vulnerable population. *Action Research*, *15*(2), 161–176. https://doi.org/10.1177/1476750316630387

Gerezgiher, H. (2017). *An Investigation of Current Status of IT Disaster Recovery Plan in Ethiopian Banking Sector*. http://etd.aau.edu.et/handle/123456789/29/browse?

Ghannam, M. Z. (2017). *Challenges and Opportunities of Having an IT Disaster Recovery Plan*. http://www.diva-portal.org/smash/get/diva2:1117263/FULLTEXT01.pdf

Goundar, S. (2012). *Research methodology and research questions*.

Grover, V. (2015). *Research Approach: an overview*. *February*.

GSMA. (2019). *Mobile Telecommunications Security Threat Landscape*. *January*, 1–20.

Gustafsson, A. (2018). *Customer satisfaction with service recovery*. *July*. https://doi.org/10.1016/j.jbusres.2008.11.001

Hagemann, J., Aburto, M., & Rose, S. (2003). WHAT IS INFORMED CONSENT? In *Informed Consent in Human Subjects Research* (p. 22). http://oprs.usc.edu/files/2013/04/Informed-Consent-Booklet-4.4.13.pdf

Hassan, L. (2017). *Information Technology Disaster Recovery Plan (IT DRP) Framework–A study on IT Continuity for Smart City in Abu Dhabi Smart Government*. *July*. https://bspace.buid.ac.ae/handle/1234/1120

Hawkins, S. M., Yen, D. C., & Chou, D. C. (2000). Disaster recovery planning: A strategy for data security. *Information Management and Computer Security*, *8*(5), 222–229. https://doi.org/10.1108/09685220010353150

Hayes, S., Wolf, C., Labbé, S., Peterson, E., & Murray, S. (2017). Primary health care providers' roles and responsibilities: A qualitative exploration of 'who does what'

in the treatment and management of persons affected by obesity. *Journal of Communication in Healthcare*, *10*(1), 47–54. https://doi.org/10.1080/17538068.2016.1270874

Hennes, E. P. (2017). Power struggles: Estimating sample size for multilevel relationships research. *Journal of Social and Personal Relationships*. https://doi.org/10.1177/0265407517710342

Hoeber, O., Hoeber, L., Snelgrove, R., & Wood, L. (2017). Interactively Producing Purposive Samples for Qualitative Research using Exploratory Search. *CEUR Workshop Proceedings*, *1798*, 19–21.

Hoepfl, M. C. (1997). Choosing Qualitative Research: A Primer for Technology Education Researchers. *JTE*, *9*(1). https://doi.org/10.21061/jte.v9i1.a.4

Hoong, L. L., & Marthandan, G. (2011). Factors influencing the success of the disaster recovery planning process: A conceptual paper. *2011 International Conference on Research and Innovation in Information Systems, ICRIIS'11*. https://doi.org/10.1109/ICRIIS.2011.6125683

Hornby A. (2010). *Oxford Advanced Learner's Dictionary* (P. P. Joanna Turnbull, Diana Lea, Dilys Parkinson (ed.)).

ITmanagers. (2013). *Flinders University IT Disaster Recovery Framework*. *August*. http://docplayer.net/19811784-Flinders-university-it-disaster-recovery-framework.html

Iyer, G. V., & Mastorakis, N. E. (2006). Important Elements of Disaster Management and Mitigation and Design and Development of A Software Tool. *Proceedings of the 7th WSEAS International Conference on Mathematics & Computers in Business & Economics*, *2006*, 102–121.

Jessie Reed. (2019). *Types of Disaster Recovery Sites*. https://www.nakivo.com/blog/overview-disaster-recovery-sites/

Jines, J. (2018). Best Practices for Disaster Preparedness. *Law and Order*, 1–5. http://www.hendonpub.com/resources/article_archive/results/details?id=1602

Joe, A.--A. (2013). Enablers of Successful Business Continuity Management Process. *Australian Journal of Basic and Applied Sciences*, *7*(10), 86–97.

Julie, B., Susan, T., & Terry, Y. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology Volume*. https://doi.org/10.1186/s12874-018-0594

Kadlec, C., & Shropshire, J. (2010). Best practices in IT disaster recovery planning among US banks. *Journal of Internet Banking and Commerce*.

Kaspersky Security Intelligence. (2018). *Mobile Telecommunications Security Threat Landscape*. 17. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07185213/Kaspersky_Telecom_Threats_2016.pdf

Kawulich, B. (2004). Qualitative Data Analysis Techniques. *Conference: RC33 (ISA)*, *January 2004*, 96–113. https://www.researchgate.net/publication/258110388_Qualitative_Data_Analysis_Techniques/link/5550bba708ae93634ec9ed30/download

Khan, S. N. (2014). Qualitative Research Method: Grounded Theory. *International Journal of Business and Management*, *9*(11). https://doi.org/10.5539/ijbm.v9n11p224

Koech, B. K. (2016). *Evaluation Framework for IT Service Continuity and Disaster Recovery Plans: The Case in Kenya's County Governments*.

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Krocker, G. (2020). *Disaster Recovery Plan Testing: Cycle the Plan, Plan the Cycle*. https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-testing-cycle-plan-plan-cycle-563

Kumar, S. (2018). Understanding Different Issues of Unit of Analysis in a Business Research. *Journal of General Management Research*, *5*(2), 70–82.

Leidinger, W. J. (2004). *Handbook for Information Technology Security Risk Assessment Procedures*.

Luckey, T. S. (2009). Key Stages of Disaster Recovery Planning for Time-critical Business Information Technology Systems. *University of Oregon*, *1277*(February 2009).

Makwae, E. (2018). *An assessment of disaster recovery planning : A strategy for data security*. *September*. https://www.researchgate.net/publication/327572587_An_assessment_of_disaster_recovery_planning_A_strategy_for_data_security

Marek, Z. (2013). *Business continuity/disaster recovery*. 1–18. https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Mark Flesch. (2019). *Developing a Disaster Recovery Plan — 5 Essential Elements*. https://www.gflesch.com/blog/essential-elements-for-developing-a-disaster-recovery-plan

Mark Pelt & Tom Baker. (2017). *Five Steps to Effective Disaster Recovery Planning*. https://advancedtechnology.com.au/disaster-recovery-planning/

Martin, B. C. (2002). Disaster Recovery Plan Strategies and Processes. Retrieved from http://www.sans.org/reading_room/whitepapers/recovery/disaster-recovery-plan-strategiesprocesses_564

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, *2*. https://doi.org/10.1177/2333393615597674

Mishra, D. S. B., & Alok, & D. S. (2017). *Handbook of Research Methodology*. https://doi.org/10.1097/00003465-199001000-00018

Munteanu, A., Fotache, D., & Dospinescu, O. (2008). *Information Systems Security Risk Assessment. Harmonization with International Accounting Standards*. *January*. https://doi.org/10.1109/CIMCA.2008.26

Namey, E., Guest, G., McKenna, K., & Chen, M. (2016). Evaluating Bang for the Buck: A Cost-Effectiveness Comparison Between Individual Interviews and Focus Groups Based on Thematic Saturation Levels. *American Journal of Evaluation (AJE)*. https://doi.org/1098214016630406

Nicodemus, B., & Swabey, L. (2015). *Action Research: Researching translation and interpreting*. *18*(1), 171–196. https://doi.org/10.21608/jfss.2020.106049

O'toole, E., Feeney, L., Heard, K., & Naimpally, R. (2018). *Data security procedures forresearchers*. *August*, 14. https://www.povertyactionlab.org/sites/default/files/documents/Data_Security_Procedures_December.pdf

Omar Alhazmi & Yashwant Malaiya. (2012). *Assessing Disaster Recovery Alternatives: On-site, Colocation or Cloud*. *May 2014*, 3–5. https://doi.org/10.1109/ISSREW.2012.20

Pamela, B., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report Volume*, *13*(4), 544–559. https://doi.org/10.2174/1874434600802010058

Pamela, E. B., & Jack, S. M. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*

Volume, *13*(4), 544–559. https://doi.org/10.2174/1874434600802010058

Paré, G. (2004). Investigating Information Systems with Positivist Case Research. *Communications of the Association for Information Systems*, *13*(February). https://doi.org/10.17705/1CAIS.01318

Partio, A. (2017). *Data Center Disaster Recovery & Major Incident Management*. https://www.theseus.fi/bitstream/handle/10024/135950/Partio_Aliisa.pdf?sequence=2&isAllowed=y

Parveen, H., & Showkat, N. (2017). *Research Ethics*. *August*.

Periasamy, K. P., Charissa, L. M. L., Wei, T. N., & Michelle, X. Q. (2016). Portfolio-based approach for disaster recovery planning for IT. *PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises*, 396–410.

Poskiparta, S. (2018). Creating a basic tool for Disaster Recovery Planning. *Creating a Basic Tool for Disaster Recovery Planning*, *Mar*. https://www.theseus.fi/bitstream/handle/10024/142539/Masters_Thesis_Simo_Poskiparta.pdf?sequence=1

Pritchard, S. (2019). *Five essential steps to a sound disaster recovery plan*. https://www.computerweekly.com/feature/Five-essential-steps-to-a-sound-disaster-recovery-plan

Qutoshi, S. B. (2018). Journal of Education and Educational Developement Discussion Phenomenology: A Philosophy and Method of Inquiry. *Journal of Education and Educational Developement*, *5*(1), 215–222.

Rahman Mohamed, H. A. (2014). A Proposed Model for IT Disaster Recovery Plan. *International Journal of Modern Education and Computer Science*, *6*(4), 57–67. https://doi.org/10.5815/ijmecs.2014.04.08

Rahman, Z. U. (2017). GSM Technology: Architecture, Security, and Future Challenges. *International Journal of Science Engineering and Advance Technology*, *5*(1), 70–74.

Rajasekar, S. P. P. V. C. (2018). Research methodology. *Constitutional Politics and the Judiciary: Decision-Making in Central and Eastern Europe*, 8–31. https://doi.org/10.4324/9780429467097-2

Rebolj, B. (2013). The case study as a type of qualitative research. *Journal of Contemporary Educational Studies*, *1*(2013), 28–43.

Regmi, K., Naidoo, J., & Pilkington, P. (2010). Understanding the Processes of

Translation and Transliteration in Qualitative Research. *International Journal of Qualitative Methods*, *9*(1), 16–26. https://doi.org/10.1177/160940691000900103

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business Research*, *10*(2), 281–305. https://doi.org/10.1007/s40685-017-0045-z

Robb, D. (2019). Disaster Recovery Site. *Enterprise Storage*. https://www.enterprisestorageforum.com/storage-management/disaster-recovery-site.html

Rouse, M. (2015). *Disaster recovery site (DR site)*. https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-site-DR-site

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2017). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising*, *37*(4), 650–663. https://doi.org/10.1080/02650487.2017.1348329

Schiff, J. L. (2016, Julay 5). 8 ingredients of an effective disaster recovery plan. *Disaster Recovery*.

Sedgwick, P. (2014). Unit of observation versus unit of analysis. *BMJ (Online)*, *348*(June 2014). https://doi.org/10.1136/bmj.g3840

Segue Technologies. (2013). *The Three Stages of Disaster Recovery Sites*. https://www.seguetech.com/three-stages-disaster-recovery-sites/

Sembiring, J., & Siregar, M. I. H. (2013). A Decision Model for IT Risk Management on Disaster Recovery Center in an Enterprise Architecture Model. *Procedia Technology*, *11*(December 2013), 1142–1146. https://doi.org/10.1016/j.protcy.2013.12.306

Shan Gupta & Changbin Gong. (2019). *Best Practices for Disaster Recovery in Oracle Cloud Infrastructure*. https://docs.cloud.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/best-practices-for-dr-on-oci.pdf

Shropshire, J., & Kadlec, C. (2009). Developing the IT disaster recovery construct. *Journal of Information Technology Management*, *20*(4).

Smith, T. (2018). *Disaster Recovery Site*. https://www.investopedia.com/terms/d/disaster-recovery-site.asp

Snedaker, S. (2007). Business continuity & Disaster Recovery for IT Professionals. In *Syngress Publishing, Inc. Elsevier,* (Vol. 15, Issue 1). https://doi.org/10.1111/j.1468-5973.2009.00556.x

Snedaker, S. (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals.* United States of America: Syngress.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(August), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Solomon, K. (2018). *Briding the Gap between business strategy and IT strategy: Exploring Strategic Alignment GAP*.

Somasekaram, P. (2017). A Component-based Business Continuity and Disaster Recovery Framework. *Uppsala University*, *March*. http://uu.diva-portal.org/smash/get/diva2:1108197/FULLTEXT01.pdf

Spencer, G. (n.d.). *ICT & Communications Services Disaster & Recovery Plan with*.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2. *NIST Special Publication 800-82 Rev 2*, 1–157. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-82r1

Sueb, S. (2013). The Development Of Technology For Human Civilization. *The Third Basic Science International Conference - 2013*, *November 2013*, 1–5.

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. *NIST Special Publication 800-34 Rev. 1*, *May*, 150.

TechTerms. (2020). *Framework Definition*. 1–2. https://techterms.com/definition/framework

Telecom Excellence Academy. (2017). *Core Components of Business Continuity Plan*.

Theofanidis, D., & Fountouki, A. (2018). Limitations and Delimitations in the Research Process. *Perioperative Nursing*, *7*(3), 155–162. https://doi.org/10.5281/zenodo.2552022

Uddin, M., Hapugoda, S., & Hindu, R. C. (2015). Disaster recovery framework for commercial banks in Sri Lanka. *Journal of ICT Research and Applications*, *9*(3), 263–287. https://doi.org/10.5614/itbj.ict.res.appl.2015.9.3.4

Umanailo, M. C. B. (2019). *Overview of Phenomenological Research*. *September*. https://doi.org/10.31222/osf.io/4t2fv

Van Hulst, M., Koster, M., & Vermeulen, J. (2015). Ethnographic Research. *Encyclopedia of Public Administration and Public Policy, Third Edition*, *June 2016*, 1–5. https://doi.org/10.1081/e-epap3-120051222

Witting, M. (2012). *Detecting Disaster Root Causes A Framework and an Analytic Tool for Practitioners*. dkkv.org

Wolgemuth, J. R., & Agosto, V. (2019). Narrative Research. *The Blackwell Encyclopedia of Sociology*, *July*, 1–3. https://doi.org/10.1002/9781405165518.wbeos1244

Yin, R. K. (1984). *Case study Research design and Methods*. https://books.google.com.et/books/about/Case_Study_Research.html?id=8U9qAAAAMAAJ&redir_esc=y

Yin, R. K. (2014). How to Know Whether and When to Use the Case Study As a Reserach Method. In *Case Study Research Design and Methods* (pp. 1–25).

Yin, R. K. (2017). Case Study Research and Applications. In *Case Study Research and Applications: Design and Methods* (Sixth).

Zhang, X., & McMurray, A. J. (2012). Embedding Business Continuity and Disaster Recovery within Risk Management. *SSRN Electronic Journal*, *3*(3), 61–70. https://doi.org/10.2139/ssrn.2174785

APPENDIX_A: UNIVERSITY COOPERATIVE LETTER WRITTEN TO CASE COMPANY ETHIO TELECOM

To:- Ethio Telecom
Addis Ababa

Dear Sir/Madam,

Student Asefa Alemu (ID.No GSR/5441/11) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "A framework of Information Technology Disaster recovery plan (ITDRP) for Ethio Telecom".

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

With Regards,

Tibebe Beshah (PhD)
Head, School of Information Science

SCHOOL OF INFORMATION SCIENCE

✉: 1176 ☎: +251-(11)-122-91-91

APPENDIX_B: SSI OBJECTIVES DECLARATION, SSI PROCEDURES AND SSI QUESTIONS

The semi-structure interviw objectives declaration

Addis Ababa University
College of Natural and Computational Science
School of information science

Dear Madams/Sirs,

My name is Asefa Alemu Degefa and I'm a post graduate student at Addis Ababa University in the School of Information Science, department of Information Science and Systems (Information Systems track). Currently I am attending my master's thesis entitled **"Developing a Framework of Information Technology Disaster Recovery (ITDRF) for ethio telecom".** IT disaster recovery plan is one of the fundamental components of BCP implemented to prevent business interruption during and after serious disasters. ITDRPF is a guideline to activate the IT disaster prevention mechanisms so as to realize a BC in a given organization. For this peculiar advantage ITDRP is a must for telecom companies to keep their mission critical day to day activities alive during and after disastrous circumstances. The focus of this thesis is the telecom industry in general specific to Ethiopian telecom service provider "ethio telecom".

From many staff members of ethio telecom you are purposefully selected to participate in this study because I the researcher believed on your all sides of experiences on IT services in telecom are very fit for this case study thesis. Since participating on this study is absolutely dependent on voluntary you have been requested orally for your agreement before this objective notification. Thank you once again being you showed cooperativeness and willingness to be part of this study. Your oral agreement is still considered, however if you thought that you don't have to answer some questions on the spot of the interview session you still have a full privilege to ignore and request me to jump it, and continue the impending question. Because of the potentially sensitive

nature of the study, every effort has been made to protect your anonymity. The data collected from the interview will be kept on the researcher's computer with high protection mechanisms. The data will never be shared with others without your prior agreement. This is to justify you that this investigation is only for academic purpose; hence researcher can approve you that there are no pre known risks from your contributions on this study. For further validation on transparency the report of this study's findings will be given to each individuals who participate in the interview. I am happy because you are with me investigate the gap on ITDRPF situation at (**ours**) ethio telecom.

For further clarifications, suggestions, questions or any concerns regarding to this study please contact me at (asefa.alemu@aau.edu.et /asefaalemu92@gmail.com and you can call me at +251930011697).

The objective of this semi-structure interview in detail are

1. To find out how companies can manage ITDRP gaps so as to realize smooth service delivery and data protection.
2. To identify the concept of ITDR in the company
3. To understand critical factors that enable and inhibit ITDRPF.
4. To investigate whether ITDRP gap exists in your company.
5. To investigate the reason why ITDRP gap exists in your organization and
6. To distinguish best ways to have ITDRP by applying best ITDRPF

SSI Procedures

A. Self-introduction to contributor.
B. Thanking contributor for accepting to participate in the study.
C. Highlight purpose of the semi-structure interview shortly.
D. Announce and acknowledge respondent that interview is being recorded based on importance.
E. Activate recording electronic material.
F. Start interview with question number 1; follow through to final question.
G. Continue to record and stopping recordings depending the importance & relevance answer.
H. End interview and give chance to add any important points if he/she has.

I. Thanking the contributor for participating in the study.
J. Confirm the contributor has contact information for follow up questions and concerns.
K. End procedures/protocols.

SSI QUESTIONS

To detect whether gaps related to ITDRP exists in the case company ethio telecom

1. Could you please explain me why your company doesn't have ITDRP?
2. Starting from your employment till this interview session have you ever been faced with some happenings which your company had/can categorized them as disasters? If there is could you, please tell me in detail?
3. Does your division/department perform RA? If yes could you, please explain in detail?
4. How do communications go in your company purposed to service restoration from any outages?
5. Which type of task is operationalized in your organization related to service interruptions from this two choices (1 Proactive 2. Reactive)? Please explain me why you say so?
6. How do you explain your knowledge towards ITDRP?

To identify challenges to attain ITDRPF in the case company ethio telecom

1. What is the biggest challenge associated with having ITDRP in your Organization?
2. Could you please describe the factors that can constrain ITDRP framework in your company?
3. Do you think that convincing the top management to install ITDRP is a big challenge in ethio telecom?
4. How do you manage the service interruption specifically unplanned down time occurred in your organization?

To detect Necessity (whether the solution is necessary and critical) to the company?

1. What are the threats to your systems, data and infrastructure resources currently?
2. What are the main advantages that ITDRP can give you to attain and enhance BC in your Company?

3. Could you please explain me how ITDRP can assist your organization in protecting data and IT services?
4. Do you consider having ITDRP as time and resource consuming process?
5. Could you please explain me the importance of ITDRP framework for ethio telecom?
6. If some disaster happens, just like flood, fire or mob around and within this Addis Ababa city what is at your company hand to defend such situation?
7. Could you explain me the emphasis of having ITDRP on ethio telecom IT staffs?

To sense what the implementation strategy should it be look like

1. Could you please explain which systems should be prioritizing while deploying an ITDRP?
2. Could you please explain me how difficult is for IT staff to respond to their normal duties and follow up ITDRP activates?
3. How do you manage the service interruption specifically unplanned down time occurred in your organization currently?
4. If you have ITDRP, how do you need to operate it?
5. Does your division (department) have a clear guideline to restore service interruptions?
6. What elements do you think to include in your ITDRP to makes successful and reliable?

---END of SSI---

APPENDIX_C: URKUND ANALYSIS REPORT

URKUND

Document Information

Analyzed document	ITDRPF Development_Thesis_Final_Report_by Asefa_ Alemu_Sept_2020.docx (D79467268)
Submitted	9/20/2020 10:38:00 AM
Submitted by	
Submitter email	workshet.lamenew@aau.edu.et
Similarity	5%
Analysis address	workshet.lamenew.aauni@analysis.urkund.com

Sources included in the report

SA	**University of Addis Ababa / Nigussie Thesis draft.docx** Document Nigussie Thesis draft.docx (D70850822) Submitted by: nega.tarto@gmail.com Receiver: lemma.lessa.aauni@analysis.urkund.com	23
SA	**University of Addis Ababa / Getnet_thesis draft.docx** Document Getnet_thesis draft.docx (D73555864) Submitted by: getnetg1@gmail.com Receiver: lemma.lessa.aauni@analysis.urkund.com	4
W	URL: https://www.bsfc.ac.uk/files/files/Policies/IT_Disaster_Recovery_Plan_(Approved_06 ... Fetched: 9/20/2020 10:39:00 AM	1
W	URL: https://talentedge.com/blog/7-things-disaster-recovery-plan-cover/ Fetched: 9/20/2020 10:39:00 AM	2
W	URL: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1068&context=msia_etds Fetched: 12/16/2019 11:35:44 PM	3
W	URL: https://www.topresearchjobs.com/what-motivates-researchers-towards-higher-performance/ Fetched: 9/20/2020 10:39:00 AM	1
SA	**FinalVersion-MohamedZiyadGhannam.pdf** Document FinalVersion-MohamedZiyadGhannam.pdf (D29085433)	16
W	URL: https://www.theseus.fi/bitstream/handle/10024/135950/Partio_Aliisa.pdf?sequence=2& ... Fetched: 9/20/2020 10:39:00 AM	3
W	URL: https://www.researchgate.net/publication/342642908_Information_Technology_Disaster ... Fetched: 9/20/2020 10:39:00 AM	1
SA	**MasterThesis-Mohamed Ziyad Ghannam.pdf** Document MasterThesis-Mohamed Ziyad Ghannam.pdf (D28823554)	4
W	URL: https://esource.dbs.ie/bitstream/handle/10788/1794/mba_bilczynska_a_2014.pdf?seque ... Fetched: 10/29/2019 12:40:36 PM	3