ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN (ITDRP) FRAMEWORK FOR BANKS IN ETHIOPIA

By

NIGUSSIE TARIKU

JUNE, 2020
ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN (ITDRP) FRAMEWORK FOR BANKS IN ETHIOPIA

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science and systems (*Information Systems specialization)*

By: **NIGUSSIE TARIKU**

Advisor: **LEMMA LESSA (PhD)**

JUNE, 2020

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN (ITDRP) FRAMEWORK FOR BANKS IN ETHIOPIA

By: **Nigussie Tariku**

Name and signature of Members of the Examining Board

Lemma Lessa (Ph.D.) Advisor	_____ Signature	_____ Date
Temtim Assefa (Ph.D.) Examiner	_____ Signature	_____ Date
Getachew Hailemariam (Ph.D.) 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 this thesis entitled "INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN (ITDRP) FRAMEWORK FOR BANKS IN ETHIOPIA" 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, Dr. Lemma Lessa. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Nigussie Tariku

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

Advisor's Signature: _____

Lemma Lessa (Ph.D.)

Acknowledgements

First and foremost praises and thanks to the Almighty God for his showers of blessings throughout my research, education and life.

I would like to express my deepest and sincerest gratitude and thanks to my supervisor Dr. Lemma Lessa without his assistance, encouragement, dedicated involvement, understanding and guidance this work would have never been accomplished.

My special thanks also goes to participants of this study at Bank A and Bank B for their friendly and professional details for the subject matter. I am grateful to my Instructors and classmates.

I am extremely grateful to my wife and children for their love, understanding, care, prayers and continuing support to complete my research work.

Nigussie Tariku

JUNE, 2020

Addis Ababa, Ethiopia

Abstract

IT services and solutions in the banking sector should be protected so as to keep the business continuing in the disastrous scenario. IT DRP ensures the provision of continuous vital business processes at an alternate site in the event of disasters. Motivated by the problem on the ground and the IT DRP framework gap identified by the previous studies in the banking sector, the researcher aimed to develop IT DRP framework for the banks in Ethiopia. The Ethiopian banks should have a mechanism and strategies in place to detect, protect, recover, reduce and avoid the likelihood that its operation will be significantly affected by such a scenario. The purpose of this study is to develop an IT DRP framework that can serve as a quality tool to help the Ethiopian Banks to evaluate their IT DRP or develop one according to their business needs. The study employed a qualitative case study method to investigate current best practices and challenges in Ethiopian government owned and private banks. A purposive sampling was used to select participants from both government owned and private banks in Addis Ababa head office. A face to face and telephone interview was conducted to collect data from both banks.

The findings from this study indicated that both Bank A and Bank B do not have IT DRP in place. Both banks are on the IT DRP project initiation stage. It was also found that Bank A has established IT business continuity and disaster recovery department which has not been established in Bank B. Lack of focused group both from IT side and management side, lack of experiences and IT DRP educated personnel in the bank and on the market, lack of training and awareness, no certified IT DRP implementation company in the country, lack of IT DRP standardization in the country, lack of guaranteed telecom infrastructure backbone are some of the challenges identified in this study. Accordingly, IT DRP framework is proposed for Banks of Ethiopia. The framework was confirmed and validated by the area experts in both banks. Recommendations are forwarded and practice and related topics are suggested for future research to extend this work.

Keywords: Business continuity, IT disaster recovery plan, disaster recovery, recovery strategies.

Publication Emerged out of this Research

Nigussie Tariku and Lemma Lessa (2020) Information Technology Disaster Recovery Plan Framework for Banks in Ethiopia. *The 6th Annual African Conference on Information Systems and Technology*. ACIST2020 virtual conference, July 02, 2020.

Note: This is a shortened version of the final thesis that was submitted to The *6th Annual African Conference on Information Systems and Technology* (ACIST2020) in the "*Completed Research Paper*" category.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ATM	Automated Teller Machine
BC	Business Continuity
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BCI	Business Continuity Institute
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BSI	British Standard International
CEO	Chief Executive Officer
CMM	Capability Maturity Model
COBIT	Common Objective for Information related and Technology
COOP	Continuity of Operations Plan
CP	Contingency Planning
CRM	Customer Relationship Management
DR	Disaster Recovery
DRIIM	Disaster Recovery International institute Model
DRP	Disaster Recovery Plan
EDI	Electronic Data Interface
EPHI	Electronic Patient Health Information
ERP	Enterprise Resource Management
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
GFDRR	World Bank and the Global Facility for Disaster Reduction and Recovery
GRR	Global Risk Report
HIPAA	Health Insurance Portability and Accounting Act
IBM	International Business Machine
ICT	Information Communication Technology

IEC	International ElectroTechnical Commission
IFRC	International Federation of Red Cross and Red Crescent Societies
IMP	Incident Management Plan
ICTRBC	Information Communication Technology Readiness for Business Continuity
ISACA	Information System Audit and Control Association
ISO	International Standard Organization
IT	Information Technology
ITDRP	Information Technology Disaster Recovery Plan
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Management
LAN	Local Area Network
MAM	Maturity Assessment Model
MTD	Maximum Tolerable Downtime
NBE	National Bank of Ethiopia
NEPA	National fire Protection Association
NIST	National Institute of Science and Standard
OTA	Treasury Office of the Technical Assistance
RA	Risk Assessment
RAID	Redundant Array of Independent Disks
RBI	Reserve Bank of India
RPO	Recovery Point Objective
RTO	Recovery Time Objective
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PTAM	Parallel Tracking and Mapping
SCM	Supply Chain Management
SEI	Software Engineering Institute
SLA	Service Level Agreements
SP	Special Publication
WBO	World Bank Organization

WEFGRR	World Economic Forum Risks Report
WMA	World Medical Association
Y2K	Year 2000’s

CHAPTER ONE: INTRODUCTION

This chapter presents an overview of the study. It provides background of the study, the background of the organization, statement of the problem, research questions, objectives of the study, significance of the study, the scope of the study, and organizations of the study.

1.1. Background

Disaster recovery (DR) is defined as a recovery of critical technology assets in the catastrophic IT failure events. IT Disaster recovery can include the recovery of each critical system that occurred in the IT environment. Disaster recovery (DR) is a part of a business continuity (BC) management program (Protiviti, 2015). Business Continuity (BC) in IT is the uninterrupted availability of IT resources that support key business functions. According to the Business Continuity Institute (BCI), business continuity is a general term that includes disaster recovery. As stated by BCI, the two terms are used interchangeably in IT to refer to the ability to recover from a disaster or unexpected event. Most of the literature refers to the BC and DR as IT BC/DR for short. The interest in BC and DR has shown much increase in the last few years, especially with the increasing corporate dependence on computer systems and the growing levels of devastation associated with recent disasters.

The purpose of this study is to identify the gap in the Ethiopian banks' disaster recovery planning practice and propose a framework that can guide them in their IT Disaster planning endeavor.

DRP is a term used to describe the recovery of technology-based resources such as applications, data, network connectivity & IT peripheral/hardware (Swanson, M. et al., 2010). DRP can be distinguished as more a tactical document that provides a short-term plan to deal with IT-specific disruptions to an organization such as cyber-attack or system failures. DRP concentrates not only on the mitigation of the disaster but also to respond to and recover IT systems. (Randeree, et al, 2012), the history of the relationship between IT BCM and DRP started in the early 60s & 70s when companies began to store backup copies of their critical data. Now, DRP is perceived as a subset of the overall BCM program and often used interchangeably with BCP. BCM practitioners

should implement their BCP & DRP interchangeably in their organization with this context though they also must understand the distinct difference between these two frameworks.

Per NIST Special Publication 800-34 Rev. 1, DRP applies to the disruption of service that causes denial of access to the primary facility infrastructure for an elongated period of time. An IT disaster recovery plan is an IT focused plan designed to restore operation of the intended systems, applications, and computed facility infrastructure at an alternate site after a disaster. A mission critical or essential business processes functions of BCP or COOP (Continuity of Operations Plan**)** can be supported by DRP by recovering such supporting systems at an alternate location. IT DRP also deals with information system (IS) disruptions that require relocation (NIST, 2010).

The causes of disaster recovery are multifold. Some of the disasters that can cause damage to an organization are fires, floods, tornadoes, hurricanes, wind and ice storms, severe storms, wildfires, landslides, avalanches, tsunamis, earthquakes, volcanoes, security incidents, equipment failures, power failures, utility failures, arson, pandemics, sabotage, strikes and work stoppages, shortages, civil disturbances, terrorism, war etc. Those incidents have the potential to cause damage to buildings, equipment, and IT systems. They affect, kill, injure, and displace and prevent them from reporting to work. Disasters also affect organizations in one or another way. The effects can be direct damage of buildings, IT equipment, and IT systems, causing buildings uninhabitable and systems unusable. There is also a utility outage that can cause no direct damage. But the essential supplies such as power, water, and others are interrupted to wider areas for days or so. Public transportation such as highways, roads, bridges, railroads, and airports are affected by widespread incidents occurring in the region. There can be communication disruption, evacuation, and workers' absenteeism. In most cases, businesses simply can't survive after experiencing such an outage that causes them to cease operations for hours, days, or longer and this is a big loss for businesses like banks. (Gregory, 2013).

The major benefits of DRP are improved business processes, improved technology, fewer disruptions, higher quality services, and competitive advantage. A DR plan allows an organization for better availability and reliability of services. Businesses do expect these benefits if and only if the development of disaster recovery plans are in place. In today's environment, most organizations depend on systems and online transaction processing. Hence, data for a few seconds can lead to million-dollar losses to an organization. Therefore, most CEOs and Board Directors of

Banks are well-concerned about having a proper contingency plan in order to face various types of natural disasters and planned terrorist activities.

According to Haylay (2017), the modern sense of banking service in Ethiopia began towards the end of Emperor Minilik II. And the first bank was opened in 1906 E.C in cooperation with the British owned National Bank of Egypt and it was called the Bank of Abyssinia. Currently, there are 16 private and 2 governmental owned banks and one central bank in Ethiopia that transact millions of birr per day. There are emerging private and government banks under development but they are not functioning yet. The main functions of banks are to give flexible money transaction services for the customers and organizations continuously, but there are natural and manmade disasters that could prevent the banks from performing their tasks normally. Nowadays banks are coming up with highly sophisticated technologies in order to get competitive advantages over their rivalries. But this is not enough for banks to stay in the market for a long time, because natural or manmade disasters could disrupt their business process and the whole system for an extended time. So banks need to adopt BCPs and disaster recovery strategies to avoid intentional or unintentional problems that prevent the system from operating its normal business processes.

Therefore, this study will help the Banks of Ethiopia to avoid certain risks or mitigate the impact of unavoidable disasters by minimizing potential economic loss and disruption of mission-critical functions, decreasing potential exposures, and recover operations quickly and successfully by developing a tailored proposed framework. The framework will also help the Banks in the event of a disaster by introducing a good plan that reduces disruptions to operations. It also ensures business stability and assists in identifying and handling critical and sensitive systems. The framework will provide a pre-planned recovery document that minimizes decision-making time, eliminates confusion and reduces the chance of human error and satisfies regulatory requirements, if and where applicable.

1.2. Statement of the problem

Continuous business is vital for any organization in order to survive in a competitive environment. It is even critical when we consider the organizations dealing with financial services and online data processing, where a fraction of a minute may be worth several millions of dollars. In today's environment, most organizations depend on systems and online transaction processing. Hence, data for a few seconds can lead to million-dollar losses to an organization. Therefore, most CEOs and Board Directors of Banks are well-concerned about having a proper contingency plan in order to face various types of natural disasters and planned terrorist activities. One incident that drew the attention of the international community towards disaster recovery were the 9/11 attacks of the World Trade Centre twin towers in New York in the year 2001. This incident forced governments of every country to emphasize the significance of disaster recovery strategies to their key organizations. The International Federation of Red Cross and Red Crescent Societies (IFRC) found 7184 disasters from 2000 to 2009, ranging from the Bhopal disaster, the tsunami in Indonesia in 2004, hurricane Katrina in 2005, the Haiti earthquake in 2010 and the Chernobyl explosions to the September 11th attack on the World Trade Centre in New York. They caused an estimated 986,691 million dollars of economic damages, millions of casualties while billions of people were affected. (World Disaster report, 2010).

Kadlec and Shropshire (2010) found that 60% of United States companies don't have IT disaster recovery plans in place. The IT disaster recovery planning guides developed were inconsistent or complicated and the resources were not complete. It was also reported that on the IT DR planning practices of 154 banks in the United States, organizations with adequate IT disaster recovery plans do not have an IT budget and IT department size was small.

In a study by Uddin and et.al. (2015) in banking and the financial sector, it was found that 59.7% of the functions are mission-critical in the financial industry and 32.3% of the mission-critical activities need a recovery time objective (RTO) of less than 4 hours. Furthermore, 96.9% of the functions should be recovered within less than 72 hours. According to a survey done by Balouris, S. (2009) on Disaster Recovery Journal for the state of business continuity preparedness, it was found that approximately 90% of the organizations were getting executive-level support for BCP and DR. But only 23% of the top-level executives thought of BCP and DR as top-level critical activities.

According to the National Bank of Ethiopia (2019), Ethiopian Banking institutions introduced various new products and services on the local market in order to gain a competitive edge among the internal as well as global players. These products mainly included new credit facilities, saving schemes, project financing tools, investment banking tools, mobile banking, and new e-banking facilities. Consequently, the operational risks in the banks are exposed due to large dependency on automated systems and centralized databases have become critical. The Basel II Framework identified broad types of operational risk events having the potential to result in substantial losses which included continuity risk events such as damage to physical assets, business disruption and system failures, loss on the account because of external fraud such as computer hacking, etc. Ethiopia is amongst the developing countries that are most vulnerable to natural and man-made disasters. Among others, flood, landslide, infrequent earthquakes and wars are the major triggering events that, over the past many years, have been causing suffering to communities and millions of dollars worth of property destructions (Basel II, 2009). A study by Mohammed (2009) showed that 54.8 % of the companies faced a disaster in their computer systems, and infrastructure threats found to be the largest cause, and the software was the most affected part. In the same study, data compiled from respondents through the questionnaire revealed that 76.3% of the companies had the plan, but did not follow all the necessary procedures and components of the plan. Nigussie (2017) on his study assessed IT disaster recovery practices in the commercial bank of Ethiopia and found that there is an ITDRP framework gap. According to Haylay (2017), the study found that 42.1% of the banks implemented ITDRP in place; whereas 57.9% of the banks didn't put it to work so far due to lack of ITDRP framework and are on pending status. However, 42.1% of banks who have the plan in place are still supposed their plan is not real as it needs major technical improvements to meet its intended purpose. As the findings of this research, the researcher concluded that ITDRP is not exercising well at Ethiopian banks due to less emphasis given to it from the top managers and inexperienced of severe disaster to strike before. To mitigate those damages in line with standards and International ISO guides such as NIST, ISO, and COBIT, a contextualized IT Disaster Recovery framework should be in place and banks should follow those guides to develop IT DRP and BCP that satisfy their needs and culture.

Balaouras (2009) indicated 6% of organizations are using ISO standards for business continuity, namely ISO 27001 and ISO 27002 to a larger extent and 45% of organizations have not considered ISO standards at all due to lack of decision-makers and influencers. These figures prove the fact

that a DR plan cannot be implemented exactly by using a template or guideline, but international standards can be considered and they will be helpful when creating a customized disaster recovery plan to cater to the business requirements. So that international standards should fit Ethiopian bank's context and culture and cannot be directly followed and implemented. IT disaster recovery plan has been one of the main concerns for IT management (Kappelman, McLean, Johnson, & Gerhart, 2014). An effective IT disaster recovery plan is essential for organizations to protect them from data loss (Hawkins, Yen, & Chou, 2000). According to the latest SIM study by Kappelman et al (2014), IT disaster recovery occupied the tenth place in top concerns for IT executives. Where the main purpose is to respond to any disastrous events at the earliest time possible, ITDRP can help the organization to ensure that their essential services and business processes continue operating in the event of a disaster (Hawkins, Yen, & Chou, 2000).

Around 40 to 50% of businesses that experience a major fire go out of business because most do not have an IT disaster recovery plan in place. Therefore, the ITDRP is receiving significant attention from researchers and practitioners. The previous local studies revealed, there is no IT DRP Framework developed for Banks in Ethiopia (Haylay, 2017; Nigussie, 2017). Thus, motivated by the problem on the ground and the research gap as suggested by scholars in recent related works, the researcher is aimed at developing an IT DRP framework for Banks of Ethiopia.

1.3. Research question

The following is the research question that will be answered in the research

- How can an IT disaster recovery plan framework be developed for Ethiopian banks?

1.4. Objective of the study

There are general and specific objectives of the study.

1.4.1. General Objective

The general objective of this research is to propose an IT DRP framework for Ethiopian Banks that can be used as a base for developing their respective disaster recovery plan.

1.4.2. Specific objective

To achieve the general objective of the study the following specific objectives are identified.

- Identifying the current practices and challenges of IT DRP in Ethiopian Banks.
- Assessing different DR frameworks which were done elsewhere in the world.
- Identifying elements of DRP per ISO, NIST, COBIT international standards and DRII models.
- Developing the proposed descriptive and prescriptive framework for Ethiopian Banks
- Evaluate the proposed feasibility of the framework by area or domain experts

1.5. Significance of the study

The proposed framework for the banks will ensure consistency of disaster recovery planning practice among Ethiopian Banks. It will increase the efficiency and effectiveness of the services provided by the banks. The practical contribution of this research is to benefit the banking sector by guiding them to develop their own DRP which will improve the business process, technology, fewer disruptions, higher quality services and competitive advantage. It will also guide banks in making adequate preparations to deal with possible business interruption scenarios.

The theoretical contribution of this research will be filling the gaps that are found in the previous researches.

1.6. Scope of the study

The scope of the study will be limited to Banks of Ethiopia and will not include other financial sectors or government and non-government organizations.

1.7. Organization of the Study

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

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

This chapter reviews different pieces of literature that are related to the objective of the study. It discusses major concepts, benefits, causes and effects, building blocks of Information Technology Disaster and Information Technology Disaster Recovery, elements of DRP, process, strategies, International standards, international and vendor based models, review the IT DRP practice in the banking sector, conceptual framework, and related works.

2.2. Disaster Recovery Plan (DRP) vs Continuity Planning (CP)

The disaster recovery plan (DRP) is an information system-focused plan designed to restore operation of the target system, critical and non-critical applications, network systems, or computer facility infrastructure at an alternate site after a disaster. There is a noticeable difference between Disaster recovery (DR) and Business Continuity (BC). IT DR refers directly to IT processes and is the process that a company will undergo when it faces a disaster or a crisis. In this process data recovery, access to important files, hardware and software rehabilitation and other activities become critical to the normal functioning of the corporate process and continuation of activities (Swanson et al. , 2010; Hoffer, 2001).

Regarding continuity plans, an organization ensures that it can survive an emergency and disaster by taking proactive measures to minimize the impact of the crises on the existing systems. CP is generally carried out before the incident actually occurs, while DR is takes place after the occurrence of the incident. CP is more strategic than DR in its execution to respond to disturbances that cover company operations which involve the people of the organization, the infrastructure, the buildings as well as the company's core services and activities (Menkus, 1994).

2.3. Causes and Effects of Disasters

A disaster causes a significant disruption in an organization's operations for a period of time. IT Disasters are caused by: Natural disasters, such as fires, earthquakes, lightning, storms, and static electricity; Software malfunctions; Hardware or system malfunctions; power outages; Computer viruses; Man-made threats, such as vandalism, hackers, and sabotage; Human error, such as improper computer shutdown, spilling liquids on the computer, and vandalism. (Gregory, 2012).

Confidential data are the prime assets owned by organizations. Events like IT infrastructure failure, server downtime, and terrorist attacks and others can cause major damage, in which case this important asset is compromised or threatened. The top 5 global risks in terms of likelihood are extreme weather events, failure of climate-change mitigation and adaptation, Natural disasters, data fraud or theft, and cyber-attack (WEFGRR, 2019 and GRR, 2019).

Technological disasters, riots, and human carnage over the years have played an equal if not a larger share in disasters. Disasters, regardless of cause, are characterized by a sudden and, for the most part, unexpected occurrence that demands timely actions to alleviate the situation. During the period when the organization relies on the new system, it runs a greater risk of disaster, perhaps a greater one than when using the old system. This is because, on top of the likely causes of system disaster, there are also risks that stem from the fact that the system is new, such as:

i). The system functions are not stabilized (both with respect to software and hardware)

ii). Frequent alterations-corrections are made to the system, hence concrete, final documentation is missing.

iii). A large number of security objects have not been completely checked or have not been implemented.

iv). Staff are not completely familiarized with the system administration nor with the available troubleshooting options (Aggelinos & Katsikas, 2011).

There are many potential disruptive events and the impact and probability level must be assessed to give a sound basis for progress. To assist with this process the following list of potential events

have been produced by Gregory (Gregory, 2012). Environmental disasters such as tornado, hurricane, flood, drought, earthquake, electrical storms, fire, subsidence and Landslides, freezing conditions, contamination, environmental hazards, and epidemic; organized and/or deliberate disruption including act of terrorism, act of Sabotage, act of war, theft, arson, labor disputes / industrial action, loss of utilities and services, electrical power failure, loss of gas supply, loss of water supply, petroleum and oil shortage, communications services breakdown, and loss of drainage/waste removal. All of the above-mentioned disaster events should be taken into account when developing a DRP to mitigate the recovery risk.

From the top ten (10) IT disasters of all time compiled by Peter Gregory (2013), it is clear that major IT contingency situations have occurred due to natural disasters causing damage to the IT infrastructure, but also by planned human activities and unexpected system failures. However, Bajgoric (2006), lists the following 6 as the most important causes for system downtime. a. Software defects/failures b. Planned administrative downtime c. Operator errors d. Hardware outages/maintenance e. Building/site disasters (i.e. fire) f. Metropolitan disasters (i.e. storms, floods).

There are several different disasters that are able to shut down business functions. The disasters can succeed in disrupting the business operations for some extended period that can result in loss of profits, loss of customers, company reputation, and company images. Organizations should reconsider having a disaster recovery plan in place as it is very difficult to understand which incident or which disaster can occur at the next moment. An excellent plan can always decrease the chances of disaster to occur and save an organization from a serious crisis. Knowing the cause will help to be proactive, prepare, and alert towards disaster (Telovations, (2012). Figure 2.1. shows that the largest (27%) of the cause is power outages. Therefore, it is best to be proactive and implement redundant power supply and options as a business solution in our disaster recovery planning. Telovations (2012) depicted the percentage of disaster causes as follows.

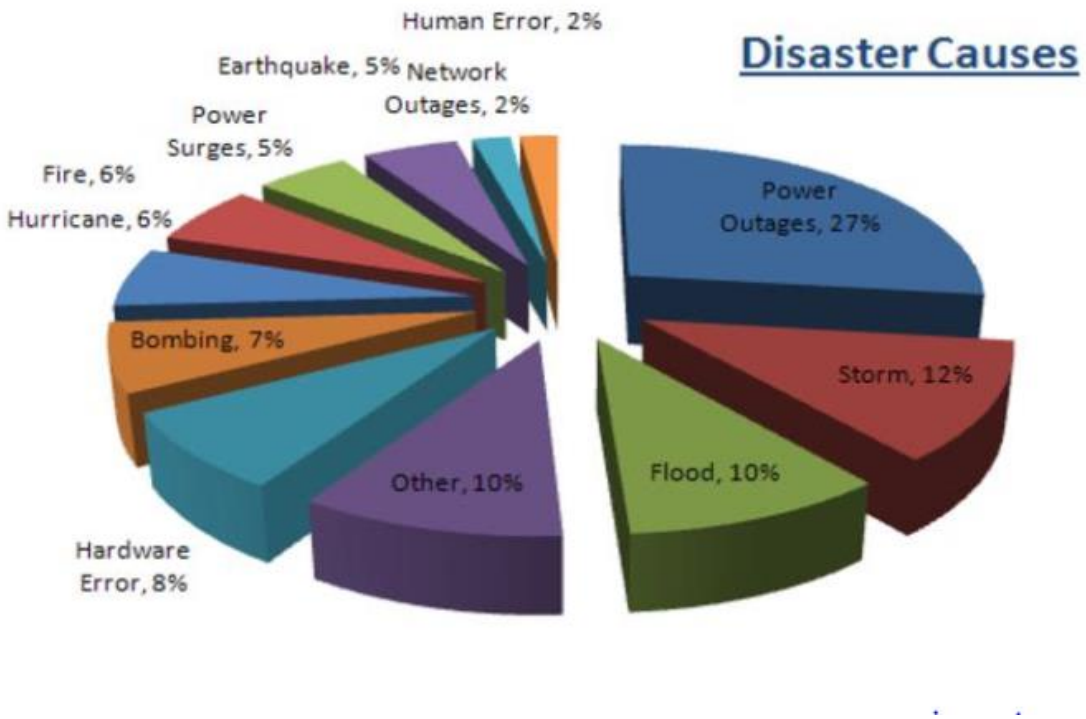


Fig. 2.1. Causes of disasters

Source: Telovations (2012).

Organizations can be affected by several kinds of disasters. Organizations like banks need to address the potential disasters that will tackle their ability to continue business operations and earn revenue. Alhazmi & Malaiya (2013) identified disasters faced by the organizations during a five years period from 2007 to 2012 and presented by the table below. This will help the company to identify potential major causes that will negatively affect its business operation and take a counter-mechanism to mitigate the causes and effects.

Cause	Organization
Power outage/failure/issues	70%
Fire	69%
Configuration change management	64%
Cyber-attacks	63%
Malicious employees	63%
Data leakage/loss	63%

Flood	48%
Hurricane	46%
Earthquake	46%
Tornado	46%
Terrorism	45%
Tsunami	44%
Volcano	42%
War	42%
Others	1%

Table 2.1. Disasters faced by organizations between years 2007-2012

Since 1980, more than two million people and over $3 trillion have been lost due to disasters caused by natural hazards, with total damages increasing by more than 600% from $23 billion a year in the 1980s to $150 billion a year in the last decade (WBO, (2019). On the other hand, investing on the more resilient infrastructure can provide a net benefit in low-and middle-income countries of $4.2 trillion, with $4 in benefit for each $1 invested, according to a report from the World Bank and the Global Facility for Disaster Reduction and Recovery (GFDRR) (2019).

It is revealed that spending on disaster recovery is almost 9 times higher than on prevention. The organizations should thus be able to respond and take swift action in the event of such attacks and catastrophes as their corporate survival depends on it. Various protocols and programs are set in place for quick recovery of data so as to protect the on-going function of the operations, securing the company's reputation. If the assets are lost however, the functioning of these companies will come to a standstill and cease to operate, resulting in them having to shut down their corporations indefinitely. Hence, IT disaster management is not an optional feature but a feature most vital to any company's protocols and a factor that can determine the success or failure of the organization depending on how effective their methods are (WEFGRR, 2019 and GRR, 2019).

The effects of a disaster on families and individuals may be long-lasting and can endure for years. However, symptoms may appear gradually, and impacts may not be seen immediately. All types of disasters are challenging, but technological disasters like the Fukushima Daiichi Nuclear Power station in Japan and previous accidents at Chernobyl tend to be even more difficult. The reason

behind this is the threat cannot be anticipated. A technological disaster is sudden, unexpected, unpredictable, and stressful. Some of the results of the effects of disasters include income loss, loss of job security, uncertainty about the future, family conflict, and stress. IT disasters affect a number of areas in financial-services-industry including the structure, the legal or regulatory environment, service delivery system, consumer and customer interests, and the safety and soundness of the banking industry (Gratten et al., 2017).

Some of the key IT disaster emergencies declared in countries and companies from around the world and its effects are the crash of computer systems globally with the beginning of the year 2000, widely known as the Millennium Bug which occurred globally and caused an estimated amount of £400 billion on the recovery operations as projected by the house of commons. IT emergencies due to failure of the system to accommodate the huge influx of visitors to access health care facilities which causes health care services disruption leading to heavy dependency of the users on outdated technology in the USA are some of the examples of IT failures that affect the world. The details are described in the table in **Appendix B** page 85 for your reference.

Source: (Barker (2017); Financial Review (2017); ACCA (2019); Financial Review (2019); CNN)

2.4. Benefits of DRP for Organizations

DRP basically helps organizations in restoring lost data and recovering data that has been lost in the process of a calamity. There are several benefits to this process.

- ✓ It eliminates confusion and human error. This can be done by giving only specific tasks to the responsible teams during the disaster. Other management teams can then focus on different matters at hand that are critical to the recovery operations. Managers are usually focused on customer service, company liabilities, vendor management, inventory, staffing, and other legal issues at this time.
- ✓ It reduces corporate interruptions during operations. While a new corporate site can be established, the corporate can presume its activities almost immediately, with the appropriate team ready and capable for the task.

- ✓ It provides alternative options for managers to consider. Before disaster strikes, the DRP can essentially provide different alternative scenarios for administrative teams to consider for recovery.
- ✓ It reduces dependence on certain key individuals. Supposing a LAN Network is destroyed in the disaster, the key personnel in-charge of handling the recovery task may be the only one who will have the knowledge in fixing the error. As such, if the personnel is not available, it can cause problems in fixing the error, which is why more than one person should be given the responsibility to handle such scenarios as one can cover for the other.
- ✓ It protects the data of the organization, which is the most valuable asset of an organization. They are stored in numerous different forms such as databases, spreadsheets, documents, and other means. They may also be more important information such as customer databases, financial documents, mailing lists, and EDI forms from vendors and customers. It is possible for users to store these data dumps in magnetic media such as tapes or hard drives and even on LAN servers. Especially for companies that are located in high-risk areas such as near water-bodies and other such environmental risks the DRP protocols become a fundamental need, with fail-safes such as elevated surfaces as well as wall-mounted racks for holding the necessary electrical equipment.
- ✓ In order to make sure that the personnel remains unharmed, the corporate offices need to be relocated to safer locations. DRP protocols can also accommodate logistical needs to transport employees from one place to another when disaster strikes.
- ✓ DRP can effectively help in a more precise and orderly recovery since critical incidents can be taken care of faster and more efficiently, giving manager's ample amount of time to focus on more stressing matters.
- ✓ Chances of Surviving can be much improved**.** No organization is reluctant to the effects of natural, technological and man-made disasters. So that having IT DRP in place improves the chance of surviving.
- ✓ Process improvements can be achieved**.** IT DRP helps to improve the processes and procedures that support the most critical and essential activities in an organization.
- ✓ Technology can be improved. This is achieved by performing the Business Impact Analysis (BIA) and establishing key metrics such as the Maximum Tolerable Downtime (MTD),

Recovery Time Objective (RTO), and Recovery Point Objective (RPO), that can make key decisions to improve the architecture of IT systems.

- ✓ Availability and Quality of systems and networks are high**.** Changes and improvements could be made through improvement of storage systems, servers, hardware, change management process, configuration management capabilities, server cluster utilization, and power management systems.
- ✓ Disruptive events can be reduced. Improving the resiliency of the IT systems that support critical business processes is one of the major aims of disaster recovery planning. This leads to fewer disruptions of those business processes when these events occur. Hard drive failure, power supply failure, short power outage, extended power outage, fire in the data center, earthquake and any disaster scenarios are reduced.
- ✓ Complying with Standards and Regulations. Regulatory bodies started to urge companies to develop the DRP plan to survive after a disaster. Accordingly, disaster recovery planning has been required by standards and regulations.
- ✓ Competitive Advantage**.** Organizations are in a state of an endless competitive struggle against each other in the global market. More and more organizations are going global and adopting processes that require continuous availability, reliability and service levels becomes an ultimate necessity. Although businesses need to be more and more available, disasters continue to occur, many of which one has no control over and this is achieved through disaster recovery planning that customers can rely on and benefit most. Therefore, IT DRP can become a competitive differentiator for organizations with strong DR plans (Hawlins et al., 2000 and Peter, 2009).

2.5. Key Stages of IT DRP

As revealed by review of the literature, there are five stages which are potentially identified and most importantly relevant to DR planning. The five DR planning stages are Project initiation, BIA, develop DRP plan, test the plan and maintain the plan (Luckey, 2009).

A. Project Initiation. In this stage, the need for DRP should be established and the plan of process to guide the development should be defined as a primary task. This stage if effectively initiated and planned also ensures the success of the resulting disaster recovery plan. Securing management help, organizing the planning project teams, establishing the project management process, getting the required resources and developing the initial project objectives are some of the major tasks of this stage.
B. Conduct Business Impact Analysis (BIA). In this stage, the IT systems of a company that must be included in the plan are determined. The priority of the critical and non-critical systems that needs to be recovered and its orders are also determined at this stage. Gathering information, identifying critical and essential IT systems, performing IT risk assessments, determining the order of recovery are some of the activities performed in this stage.
C. Developing a DR Plan. Identifying and documenting each and every procedures and policies that are used in the event of crisis are needed to be done at this stage. The activities and tasks required to develop a magnificent DRP plan include but are not limited to selecting risk management strategies, defining crisis severity levels, identifying activation triggers, documenting specific recovery processes, and selecting disaster response team members.
D. Testing a DR Plan. After the DRP plan document has been written, it should be tested against recovery objectives defined in the BIA to ensure it accomplishes the purpose it is developed for. If the purpose is not accomplished, it should be revised and the test must be repeated several times until the objective is met. Major testing activities in this stage are developing a test strategy, training the recovery staff, conducting the test procedures, and establishing the test frequency.
E. Maintaining a DR Plan. In this stage, change and update management that directly reflects the current and continuous change of organizational business is required. The activities required in this stage includes identifying potential sources of change, selecting the change management strategy and maintaining the planning documentation.

2.6. IT DRP Elements

There are seven categories of actions. Each category has its own respective elements except backup procedures. In general, there are 16 elements identified under the seven categories. Kadlec and Shropshire (2009).

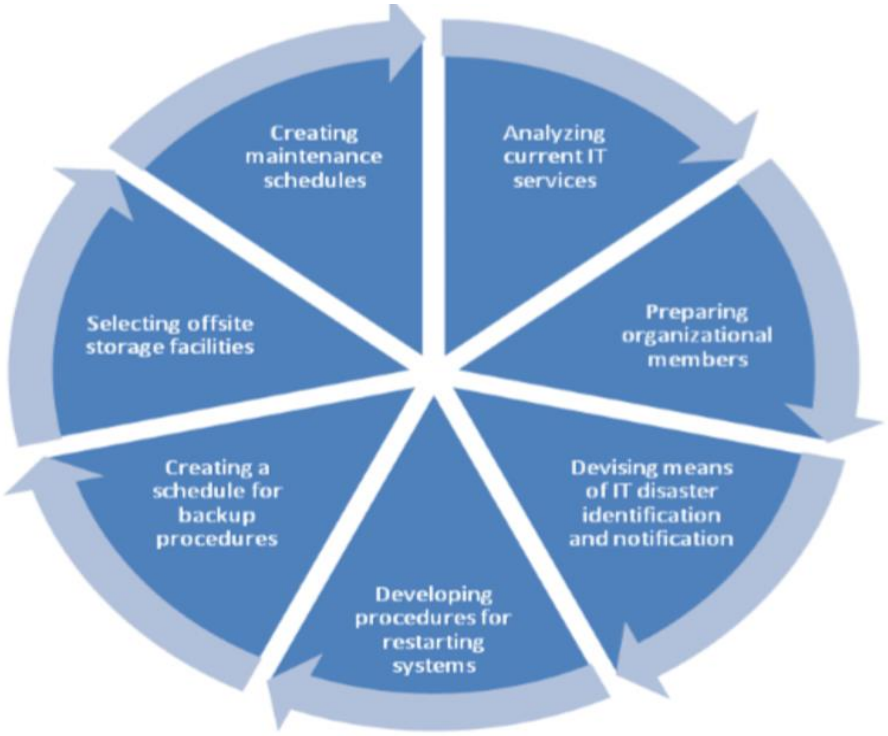


Figure 2.2. IT DRP Categories

Source: Kadlec and Shropshire (2009)

1. IT Disaster Identification and Notification. This category includes processes and procedures to detect IT related crises. It is used for communication during emergencies. IT DRP teams and shareholders are also warned during disaster using this procedure. Some of the elements identified under this category includes detection, warning and means of communication.
2. Preparing Organizational Members. This category includes sub-elements like IT DRP team training, non-team training, and formal structure of decision-making during disaster.
3. Analyzing IT Services. This category includes elements such as classifying IT and critical system services, ordering the services in terms of reactivation, and identifying potential threats and security holes.

4. Recovery Process. Under this category, initiating IT systems such as IT recovery procedures and alternative facility procedures are clearly defined and used after any IT disaster has occurred.
5. Backup Procedure. It is used for creating copies of data, network IP, software, configuration files, and the actual IT recovery plan document.
6. Offsite Storage. This category includes portability of critical and essential systems, software, configuration files and network and other data are well planned and offsite locations are selected according to known standards.
7. Maintenance. This category is where the testing, changing and updating of the IT DRP and its associated documentation is done.

2.7. Process of IT DRP

There are steps that are consistent across all BCM frameworks, models, and solutions. The following 8 processes or steps are identified from the literature. Somasekaram (2017), Acronis (2016) and Susan (2007)

1. Establish a Planning Committee. This step consists of selecting key members from various sections and departments to establish the planning committee. IT DRP plan should include a list of all important members along with their contact information, roles, and responsibilities. Those members with planned backup personal should be available in the event of a crisis.
2. Risk Assessment (RA). The next step in the pre-planning phase of IT DRP is to conduct an IT risk assessment analysis. This includes the inventory of IT equipment, IT applications, IT network and data, IT systems, servers, and software as well as identifying the mission-critical, critical, essential, and non-critical systems plus the impact the disaster has on those systems.
3. Business Impact Analysis (BIA). It is used to define appropriate MTU, RPO, and RTO for each business process or a disaster scenario. The RPO and RTO are two important metrics that are widely employed to quantify the BC/DR requirements.
4. Establish Priorities for Applications and Systems. After the mission-critical applications and systems have been determined, prioritizing them is crucial to limit the risk of extended losses and disruptions.

5. Develop Recovery Strategies. The approaches needed to implement the required resilience must be defined so as to be compliant with the principles of incident prevention, detection, response, recovery, and restoration. During this step budget, resources, suppliers, physical facilities, human constraints, technological constraints, regulatory obligations, and risks for both automatic and manual procedures should be considered.
6. Develop a Disaster recovery plan. This stage requires identification and documentation of specific policies and procedures to be used in the event of a disaster.
7. Conduct awareness, testing, and training of the DRP. Once the plan has been developed, it must be tested and audited to ensure whether it can accomplish a recovery objective or not. Major tasks include developing testing strategy, training staff and conducting testing procedures.
8. Conduct Disaster Recovery Plan maintenance and exercise. IT DR requires continuous support, update and maintenance in order to fit the current requirements. The basic tasks required to maintain the IT DRP are identify the main source changes, select change management policy and documentation of the maintaining plan.

2.8. IT DRP Strategies

The recovery strategies relocate critical IT Systems, applications, configuration files, and other data to an alternate processing location. The data and IT systems are recovered at the location of the alternate site. It should be frequently checked that the critical systems, system configurations and the associated network files and all requirements are correct and technically feasible at all times. Depending on the plan of the organization and its business strategy, a biannual, quarterly or yearly testing will take place as part of the alternate processing strategy. The associated network connectivity and physical facility will be recovered based on the extent of the disruption and crisis scenario, using the alternate recovery strategy. The emphasis of data center recovery tasks will be to recover critical applications and related processes effectively and efficiently. Critical-applications could be recovered after data center activation is whistled (Mohammed, 2014).

There are three phases of IT DR data center strategies.

Phase I: Functional Teams and Responsibilities. In this phase, the emphasis is to move the operations to the DR backup location. This activity begins after the activation of the DRP plan. The elements of this strategy includes a damage assessment team, disaster recovery team, restoration team, operation team, customer support team and major plan components.

Phase II: Disaster Recovery Action Plan. In this phase the aim is to recover the critical business systems and associated network connectivity to be able to continue the business operations minimizing downtime of the critical business functions. The elements included in this phase are backup and storage procedure, backup facility, disaster preparation, emergency response, recovery procedures and recovery time table.

Phase III: Evaluating and Testing the Disaster Recovery Plan. This is to test and evaluate if the recovery procedure to the alternate location works according to the plan. It includes testing elements such as testing the recovery plan, alternate site test procedures and planning, application test support, posttest and site test schedule as well as maintaining the plan.

2.9. IT DRP Techniques

Recovery techniques can be used to restore data in a system to a usable state. Such techniques are widely used in filing systems, applications systems, Infrastructure systems, and database systems in order to cope with failures. If a failure not only corrupts the ordinary data, but also the recovery data, complete recovery may be impossible.

Alternative site is a premise where computer hardware and network infrastructures used to process data and provide service to the user when the primary location failed to perform its usual function because of disaster strikes. There are several alternative disaster recovery sites that implement at different levels of recovery capability. The disaster recovery site can be varied from one organization to another organization depending on the business requirements and complexity. The following four main alternate site options are identified from the literature. Manhoi et. al. (2000) and Peter (2009).

Site	Description	Hardware/ Software	Network/ Communication	Failover Time	Cost
Mirrored	It provides the highest level of availability because data is written and stored synchronized at both sides.	Full	Full	Seconds	Super High
Hot Site	Mirrored setup between two data centers. It provides complete redundancy.	Full	Full	Immediately	Very high
Cold Site	Resources are allocated and pre-configured so that data can be synchronized between two sites. The resources on the secondary data center are in standby mode.	Partial	Partial	Minutes to a few hours	High
Warm Site	Only power and cooling and some other basic setups are in place. Servers and other equipment must be allocated before a recovery can be initiated in case of a disaster.	None	None	From days to weeks	Low

Table 2.2. Alternate site and its description

2.10. IT Disaster Recovery Service Level Agreements (SLAs)

The availability of a service depends on the availability of the network of data centers that host the service. This can be further expanded to include all components of an IT solution, which indicates that the availability of an application service or scenario depends on all the layers that are used to host the service. IT DR solution requires that there is a secondary site or data center that can be used to recover an IT solution in case of a failure. Because of factors such as SLAs, business requirements, technical capabilities, and disaster readiness of an IT environment, its recovery also varies. Disaster readiness implies adhering to the common standards, agreements, and technical setup regarding BC/DR, as an organization may have one set of arrangements regarding DR for all IT solutions (Goiri et al., 2011and Premathas, 2017).

The table below lists the different SLAs and how they are connected to the availability requirements. Thus, business requirements are mapped to availability and subsequently to SLAs.

Number of 9's	Availability Percentage	Total Annual Downtime	Service Level Agreements
2	99%	3.7 days	5
3	99.9%	8.8 hours	3
4	99.99%	52.6 minutes	2
5	99.999%	5.3 minutes	1

Table 2.3. Service level agreements and related availability requirements.

2.11. Audit of IT DR and Preparedness

IT Auditing is defined as the formal, independent, and objective examination of an organization's IT infrastructure to determine whether the activities (e.g., procedures, controls, ITDRP, etc.)

involved in gathering, processing, storing, distributing, and using information comply with guidelines, safeguard assets, maintain data integrity, and operate effectively and efficiently to achieve the organization's objectives. IT auditing provides reasonable assurance (never absolute) that the information generated by applications within the organization is accurate, complete, and supports effective decision making consistent with the nature and scope of the engagement previously agreed. Banks with computerized systems and IT auditors in place should have assessed threats to the system, its security holes, business impact, and loss of critical business operations would have on the bank's ability to operate and achieve its business objectives. A visible measure should be in place to reduce risks and vulnerability to a level that is acceptable to the bank's senior management and board of members. The extent of IT DRP and the detailed measures required by the banking sector vary considerably. Banks with large IT departments, mainframe computer systems and complex communication network systems could require comprehensive, up to date continuity, fascinated technology and recovery plans which incorporate standby facilities at alternative sites. At the other end of the scale, a small bank with a desk-top PC, running a simple off the shelf package, would have a simpler plan. To determine whether recovery plans for the bank sectors work as intended, the plans should be tested periodically as part of testing and maintenance exercises. The importance of adequate DRP documentation is increased where significant dependence is placed on a few key members of the Bank's IT department. The loss of key IT staff could adversely affect the bank's ability to resume operations within a reasonable timeframe. Back-up copies of systems software, configuration files, financial applications, and underlying data files should be taken regularly as needed (Angel, 2018).

The Bank's IT auditor while assessing the adequacy of disaster recovery plan should consider:

- ✓ Evaluate the disaster recovery plans to determine their adequacy by reviewing the plans and comparing them to bank's standards and regulatory bodies.
- ✓ Verify the disaster recovery plans are effective to ensure that bank data processing abilities can be resumed perfectly after disruption without affecting customers.
- ✓ Evaluate off-site storage is synchronized to online to ensure its accuracy by inspecting the facility and reviewing its contents and security and environmental controls.
- ✓ Evaluate the ability of IT and bank's customer personnel to respond effectively in emergency situations by reviewing emergency procedures, employee training and results of

their drill. Thus, IT audit, evaluation and preparedness regarding disaster recovery should be considered in Banks

2.12. Challenges of IT DRP

Organizations maintaining business dynamism and attain a competitive edge in the global scene are getting challenged due to the demanding stakeholders and keen competition. Sustaining uninterrupted business operations is key in an organization's strategic plan to maintain a competitive edge. According to a study by the University of Minnesota, 93% of firms that lose critical systems for more than 10 days file bankruptcy almost immediately; 80% of firms affected by a major incident are forced to close within 18 months (Finn et al., 2006). Anexinet (2017) identified 4 major challenges with traditional disaster recovery. The first one is a tape storage challenge. The advantage of tape storage is that it's very reliable. The demerit of tape storage is that tapes are difficult to inventory, they can be easily lost or stolen, and they are time-consuming to test. Additionally, fast restoration of applications and data after a disaster isn't possible; tapes must be recalled and restored and takes a significant amount of time. While offsite tape storage is still a reliable and affordable option for long-term off site archival and data protection, it's not the best option available today for disaster recovery, because businesses need better RPOs and RTOs than what tape can provide. The second challenge is meeting RPO or RTO. For most companies using tape backup, their RPO is 24 hours (because they do a backup each night) and the RTO might be 48 hours, because that's how long it would take them to recall the tapes, recover the data, and bring the applications back up. While that timeframe and amount of data loss might be fine for a small business, it's not going to be acceptable at medium and large enterprises. With thousands of employees working every day, the thought of losing a day's worth of data (24-hour RPO), and the cost to try to recreate that, is unacceptable. The third challenge is high costs. In the past, it's been widely known that "the shorter the RPO and faster the RTO, the greater the cost of the disaster recovery solution" (in terms of hardware, software, and data transmission). Many DR replication solutions were designed just for specific applications. All this semi-custom disaster recovery technology, plus the monthly bandwidth to support the movement of the data, resulting in a very high cost for a high-quality DR solution. Unfortunately, this put disaster recovery out of the financial reach for many companies. The fourth challenge is maintaining the IT DRP. This

plan is connected to the steps that the actual administrators would take in the event of a real disaster. It must include a plan for every application, its associated data, and user connectivity, and the sequential recovery steps for the application. With applications changing and moving at a constant rate in the modern data center, the task of maintaining disaster recovery has become overwhelming for most companies. The result is that their ITDRP is out of date, and, should a real disaster occur, they would be unable to meet the recovery time objective and maybe be unable to recover at all. This is because their maintenance plan doesn't provide the necessary information required to get the applications back up and running.

All organizations like Banks, government, higher education, health sector, private sector, and individuals must understand vandalism or loss of data can give a negative impact on the asset, quality of services and operation management. Achieving maximum security is one of the challenges these days. A security incident that will affect an asset will also have an impact on the owner of the asset (the Banks, the enterprise, or the individual). There are three major factors of security challenges in the distributed environment. These include availability issues, management and control issues and data viability issues (Mohd et al., 2014).

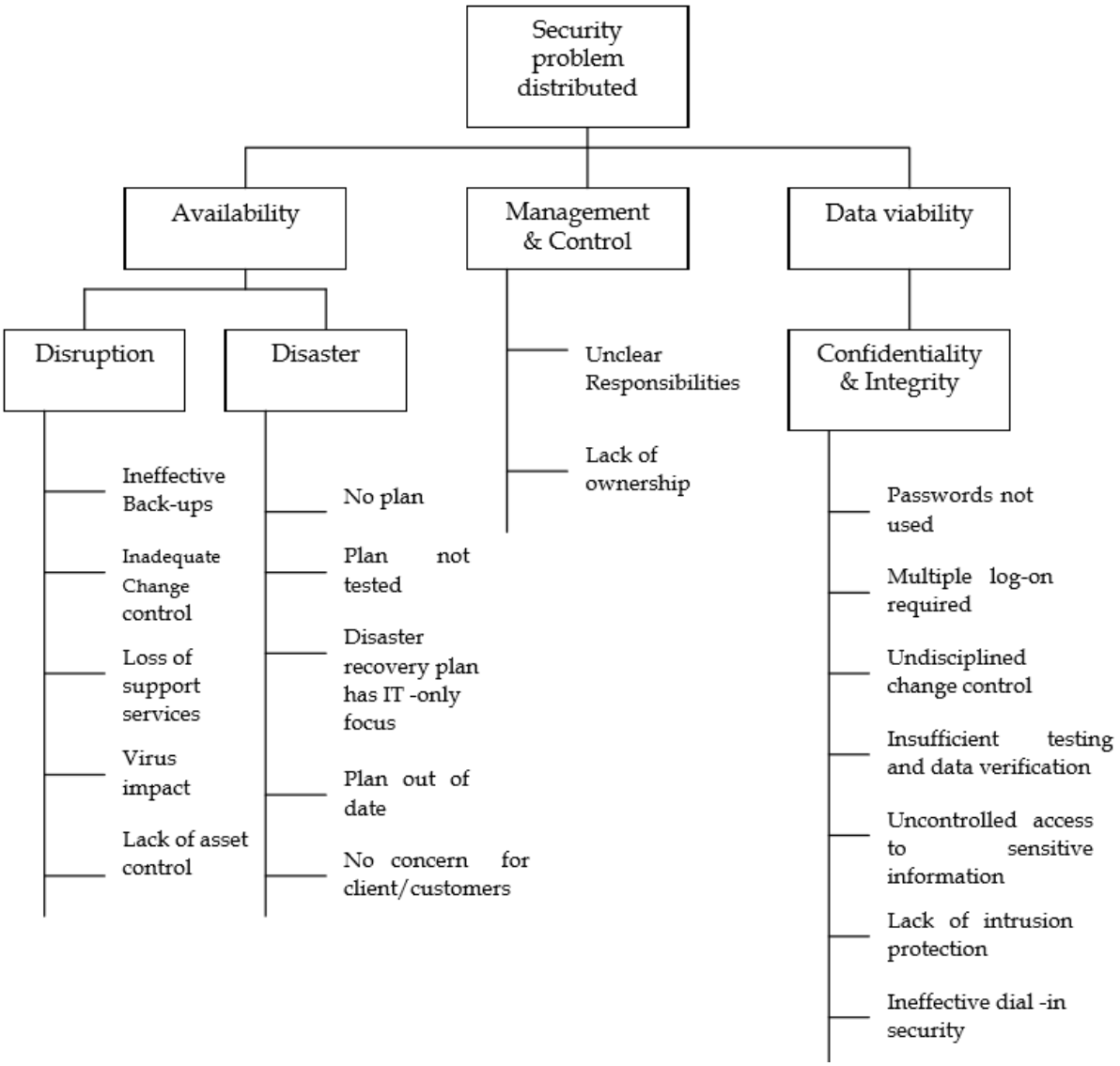


Fig. 2. 3. Security challenges in the distributed system

Source: Mohd et al. (2014)

Cybersecurity clicks on danger for disaster recovery and the universal devotion for cyber-security endures cultivating. 71.1 billion in 2014 (7.9% over 2013), and 75 billion in 2015 (4.7% from 2014) and anticipated to spread 101 billion by 2018 (Srinivasan and Simma, 2017).

Factors for effective ITDRP development such as: Top management support, Sufficient financial support, Alignment of ITDRP objectives with business goals, Conduct off-site Backup, Choosing an alternative site, Maintenance, and update of ITDRP, Continuous test of ITDRP, and Perform

Risk assessment and business impact analysis are important to consider. The challenges of adopting a disaster recovery plan includes top management support, staff issues, IT DRP maintenance, and disaster recovery site (Mohammed, 2017).

2.13. IT DR in the Financial Sector

Business disruption can happen anywhere, anytime in any financial sector. Massive tsunamis, hurricanes, terrorist bombings, power outages, and more have made recent headlines. It is not possible to predict every time what may strike even though we have all advanced technology-based systems. Today's 24x7x365 business world is running its operations with all the rest to meet the needs of the modern economy. In such a situation, it has become mandatory to prepare for any of the disastrous situations in the financial sector.

2.13.1. IT DR in banks

Banks began to use banking technology with the use of Advanced Ledger Posting Machines (ALPM) in the 1980s and Total Branch Automation (TBA) which came in the late 1980s. This automated both the front-end and back-end operations within the same branch. Lately, the new private sector banks entered into the field of automation. These banks opted for different models of having a single centralized database instead of having multiple databases for all their branches with the evolution of the ATM delivery channel. ATM, internet banking and mobile banking have improved customer convenience by providing anywhere any time banking services. The utility bill presentment and payment has helped customers to pay their bills online at the click of a button. Electronic clearing systems and electronic funds transfer have facilitated faster funds movement and settlement for the customers of different banks and different centers. In Parallel, the number of risks to IT continuously increases. The banking sector worldwide faces various types of external and domestic risks that threaten the success and long-term survival of many banks. The extreme turbulence of financial markets since September 2008, the destruction of the World Trade Centre in 2001, cyber space attacks and global terrorism have convinced many banks of the need to ensure business continuity following unexpected incidents, and to realize monetary stability. It is not possible to ignore risks to information technology. In general, IT is such an essential part of

banking business operations that it has become necessary to conduct an IT DRP on an ongoing basis (Christopher and Jordan, 2009; Al-Tamimi and Al-Mazrooei, 2007; Swartz et al., 2003).

2.13.2. IT DR in banks of Ethiopia

Ethiopia is amongst the developing countries most vulnerable to natural and man-made disasters. Among others, drought-induced famine, flood, landslide, crop-pests, infrequent earthquakes, fires, and wars are the major triggering events that, over the past many years, have been causing suffering to communities and millions of dollar worth of property destructions (Mulugeta, 2009).

According to the Ethiopian ICT Development Agency (EICTDA) (2008), Banks are categorized as critical (Level 1). At a national level, a Public or Private Institution can be considered critical to the Nation's ability to function, if any failure in their IT resources could adversely affect the ability of other Public Institutions to operate in a normal manner. This adverse effect is expected to directly or indirectly impact Citizens from receiving required services from a Public or Private Institution.

Per the report of NBE (2009), 93% of the banks did not have a disaster recovery or contingency plan in place. There is a 35% increase between 2009 and 2017. According to Haylay (2017), the study showed 42.1% of the Ethiopian banks have ITDRP in place but 57.9 % of the banks were on the way of developing the plan. The 57.9% of banks have not deployed ITDRP so far as the top managers of the banks didn't consider it as urgent, lack of skillful manpower and considering it as waste if they invest in it because they thought the environment is safe from serious disasters. Though 42.1% of the banks have the plan in place but it's far from meeting the international standards set by the different standards governing body. Nigussie (2017) found and concluded that most of the banks performed risk and business impact analysis and half of the respondents agreed that risk limitation mechanism was in place. IT disaster recovery plans of a significant number of the banks did not account for human aspects of IT disaster recovery. In addition, regular plan update and testing were the main gaps observed with a significant number of respondents not having any testing method. It was also found by the same author that the majority of the banks used cold alternate processing sites and half of the responses indicated traditional backup as data recovery solution with the same number of respondents also using daily backup frequency. RAID system, cooling, power and connectivity redundancy, and virtualization constitute the top three

system protection and resilience solutions in the banks and no bank had considered international standards in its IT disaster recovery development.

2.14. International and Vendor based Standards and Models

2.14.1. ISO

According to Guidance of BSI Standard BS ISO 22313 (2012), and most standards are associated with security, as BC/DC is an important part of security too. If an IT solution is not available due to a massive attack, a BC/DC solution can be employed to recover the solution at an alternate site. The ISO/IEC 22301:2012 and ISO 22313:2012 standards provide standards for BCM, but they do not consider DR management. On the other hand, ISO/IEC 27031:2011 and ISO/IEC 24762:2008 detail concepts and principles for DR as well, but ISO/IEC 24762:2008 has been withdrawn. Thus, ISO/IEC 27031:2011 is the only ISO/IEC standard that deals with DR to some extent. ISO 22301:2012 describes the requirements to establish, plan, implement, monitor, operate, review, maintain and continuously improve a documented management system to protect, reduce, prepare for, respond to, and recover from disruptive incidents and crises when they occur (BC Institute, 2010).

2.14.2. COBIT

COBIT stands for Control Objectives for Information & Related Technology (2014). COBIT is a framework developed by the Information Systems Audit and Control Association (ISACA) for IT management and IT governance standards. Generally accepted information technology control objectives domains include; principles, policies and frameworks, processes, organizational structures, culture, ethics and behavior, information, services, infrastructure and applications, people, skills, and competencies. It mainly supports managers to bridge the gap between control requirements, technical issues and business risks. COBIT 5 is a framework that provides a comprehensive guideline that assists the enterprise to achieve the goals and deliver values through effective governance and management of enterprise IT. However, this framework is mainly established for BCM Audit/Assurance Program and IT Continuity Planning Audit/ Assurance

Program. COBIT enables business executes to better understand how to direct and manage the enterprise's use of IT and the standards of good practices to be expected from the IT providers. COBIT 5 addresses all the management of information and related technology from an enterprise-wide and end to end perspective and includes the following 5 principles.

A. Meeting stakeholders needs
B. Covering the enterprise end-to-end
C. Applying a single integrated framework
D. Enabling a holistic approach, and
E. Separating governance from management

2.14.3. NIST

The NIST 800-34 contingency planning guide for federal information systems is a set of guidelines that outlines a seven-step process for managing BCP and DRP. NIST is responsible for developing standards and guidelines for providing adequate information security and for all operations and assets. It's created by the federal government of the US and it has a series of Special Publication (SP) Federal Information Processing Standards (FIPS) that provide federal agencies with standards and guidelines for most aspects of information systems security. NIST SP 800-34 – was the first publication for IT contingency planning guidelines and provides instructions, recommendations, and considerations for government IT contingency planning (NIST, 2010).

The seven processes for managing BCP and DRP are:

- Develop the contingency planning.
- Conduct the Business Impact Analysis.
- Identify preventive controls.
- Create contingency strategies.
- Develop an IS contingency plan.
- Testing, training, and exercises.
- Maintenance.

The step "Create contingency strategies" lists the different strategies, such as backup and recovery and alternate sites, while also considering SLAs with suppliers and vendors.

2.14.4. ITIL

According to ITIL (2016), IT Infrastructure Library is a global standard in the area of service management and the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. ITIL contains comprehensive publicly accessible specialist documentation on the planning, provision, and support of IT services. This framework also contains guidelines for the BCP process and documentation. There are five stages in ITIL service lifecycle: service design, service strategy, service operation, service transition, and continual service improvement. some of the benefits of ITIL for customers/users are: IT services are described better in more detail; quality, availability, reliability, and cost of the services are managed better; The provision of IT services becomes more customer-focused; The IT organization develops a clearer structure, more focused to the corporate objectives; The IT organization has better control of the IT infrastructure and services; ITIL provides the quality internal communication, and communication with suppliers (Kozina, 2009).

2.14.5. ITSCM

According to Cater-Steel et al. (2007), the rise of IT service management (ITSM) focuses on providing quality IT services that align IT with the business goals. ITSM is process-oriented where companies often employ software tools in order to support or automate all or part of these processes (Kuamoo, 2006). IT service continuity management (ITSCM) is one of the ITSM processes and an extension of DRP OGC's Authorized Authors (2001). In addition to being a critical technical component of BCM, ITSCM has incorporated the critical phases from BCM into the traditional DRP functions (Loftness & Drapeau, 2007). ITSCM's goal is to support BCM and ensure the businesses could have the IT systems back as quickly as possible after a disruption. In the development of version 3 of ITSM processes, four components were core: process, people, product (or tool) and partner (or vendor). It's about developing processes and procedures to manage the IT operation environment with the right product, people and vendor in place. This includes employees working on the recovery of IT services and vendors who support them. As such, an individual

component has been introduced since then to reflect the importance of people (including partners) in the process development of OGC Official Site (2008).

2.14.6. NEPA

ISACA (2012) the NFPA 1600 is from the US National Fire Protection Association, and it provides standards for disaster/emergency management and BCPs. It is devoted to eliminating death, injury, property and economic loss due to fire, electric and related hazards. NEPA 1600 standard provides fundamental criteria to develop, implement, assess and maintain the program for the prevention, preparedness, mitigation, response, continuity, and recovery. The guideline contains phases like program management, planning, implementation, training and education, exercise and tests, and program maintenance and improvements as well as respective specific elements.

2.14.7. PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS stands for payment card industry data security standard. It is an IS security standard for organizations that handle credit cards from the major card schemes. PCI DSS deals with the creation of the incident response plan to be implemented in the event of system compromise. It ensures the trust of customers with their sensitive payment card information and banks stay compliant with the standards and regulations. It also ensures the specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (PCI DSS ver.1.1 section 12.9.1, 2008).

2.14.8. BSI (British Standard International)

The British Standards Institute is one of the pioneers in developing international standards for business continuity. Their proposed standard BS25999-1:2006, includes the best practices in business continuity management (BCM) and disaster recovery. It describes the basic outlines and needs of deploying a BCM environment in order to manage the business-to-customer and business-

to-business relationships. In 2007 the British Standards Institute released another specification, namely BS25999-2:2007, widely accepted by the business community: “BS 25999-2 specifies requirements for establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and improving a documented Business Continuity Management System (BCMS) within the context of managing an organization’s overall business risks” (BSI, 2008). Sheth argued that the BS25999 standard does not discuss the survival probability of a business in a disaster situation but focuses on the implementation of a business continuity management system (BCMS) (Sheth et al., 2008). In 2008, BSI introduced another standards specification: BS 25777:2008. This was introduced as a code of practice for Information and Communication Technology continuity management. BSI has identified that not only the IT infrastructure but also the communication infrastructure is vital for the survival of a business. This guideline caters for a better framework in order to achieve a high-level preparedness for disasters.

2.14.9. Basel Committee

The Basel Committee on Banking Supervision (BCBS) is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision, and practices of banks worldwide with the purpose of enhancing financial stability. The BCBS does not possess any formal supranational authority. Its decisions do not have legal force. Rather, the BCBS relies on its members' commitments to achieve its mandate. BCBS members include organizations with direct banking supervisory authority and central banks. Disaster recovery is a huge area that covers end-to-end solutions in order to cater for contingency situations. Basel II addresses operational risk and defines it as “the risk of loss resulting from inadequate or failed internal processes, people & systems, or from external events.” The Basel Committee on Banking Supervision of the Bank for International Settlements has announced 7 main principles that an organization should follow while creating a disaster recovery solution (Bank for International Settlements, 2016),

Principle 1: Organizations should realize and emphasize the requirement of having a disaster recovery plan. Top-level senior management and board of directors should take the responsibility of having a proper contingency plan in place.

Principle 2: Management should advise the organization to have a proper DR plan in place. Principle 3: Each business group should develop its own business continuity plan considering the criticality of their contribution to the business. In this, it is vital to identify the critical systems and the tolerance level of downtime for the same. Therefore, recovery objectives can be derived.

Principle 4: Emphasize the critical importance of the internal and external communications and build up a proper mechanism in order to cater for disaster situations. This is important to build up external customer trust and confidence.

Principle 5: Highlight the importance of cross-border communications. There can be situations in which organizations have to deal with external institutions and regulatory bodies.

Principle 6: Disaster recovery plans should be well documented and they should be reviewed on a periodic basis. This can be achieved by applying periodic disaster recovery testings and drills in order to identify new requirements and changes in the existing disaster recovery plans.

Principle 7: Ensure and keep reviewing the appropriate approaches and ensuring the possibility of reaching the recovery objectives set by each business group.

2.14.10. Maturity Assessment Model (MAM)

Tipton and Krause (2007) defined a framework or model that covers the maturity of both business continuity and disaster recovery planning. The framework draws from the terminology defined by NIST Swanson et al. (2010). Tipton and Krause (2007) defined five stages of maturity for contingency and disaster planning. They include uncertainty, awakening, enlightenment, wisdom, and certainty. Along with the stages they defined a second dimension containing the five areas which are Management understanding and attitude, Contingency planning organization status, incident handling, contingency planning economics, and contingency planning improvement. This is used to alert banks at which stage their existing status is. For the description of the stages and areas please refer Appendix E page 89.

2.14.11. Disaster Recovery International institute Model (DRIIM)

According to the model developed by the Disaster Recovery International Institute (DRII), there are 10 subject areas that organizations and DR coordinators need to be thorough with. They are:

I. Program Initiations and Control
II. Risk Evaluations and Control
III. Business Impact Analysis
IV. Business Continuity Strategies
V. Emergency Response and Operations
VI. Business Continuity Plans
VII. Awareness and Training Programs
VIII. Business Continuity Plan Exercise, Audit, and Maintenance
IX. Crisis Communications
X. Coordination with External Agencies

2.14.12. Comparison of COBIT, ITIL, ISO and NIST Standards

The details of each standard have been discussed in the previous sections. Most of the IT DRP concepts or themes from the literature are similar to the themes in the international standards such as NIST and ISO for example. The weaknesses of the standards show that it is difficult to directly implement to Ethiopian context and culture without detailed consideration and a combination of the standards to overcome the limitations of the others. A comparison of major standards like COBIT, ITIL, ISO, and NIST are discussed in the table. For details please refer to Appendix F on page 95 in the Appendices section at the end of the document.

2.15. Related Works

There is no literature on DRP Framework conducted either on banks of Ethiopia or other sectors in the Ethiopian context. But there is few literature on DRP investigation and assessment made. However, related research works on IT DRP are discussed to show their similarities, differences and their limitations to this research. The methodology, results, future study and contributions are summarized in the table in Appendix G in Appendices section on page 97.

Haylay (2017) investigated the current ITDRP status in Ethiopian Banks using mixed methodology. The study found that 58% of the banks have no ITDRP in place. According to this study there is a lack of ITDR framework and standardization, the problem of ITDRP adoption, lack of top management involvement, the problem of risk identification, and management perception. Furthermore, there is no ITDRP update, maintenance, and test performed for those that developed the ITDRP.

According to Nigussie (2017), assessment of ITDRP on commercial banks of Ethiopia has been made using qualitative methods. 51% of the respondents agreed there is no risk control mechanism and 25% confirmed risks and its impacts on the bank have not been analyzed. 40% responded there is no IT DRP in place and the banks have not considered any international standards at all. Besides, IT DRP human aspect, updating, maintaining, and testing are the components that have been overlooked by those branches that implemented it. The study found and recommended the ITDRP framework as the future study. This study did not consider the private banking sector.

Both Mohammed (2014) and Uddin et, al. (2015) used a qualitative approach to develop a model for organization and ITDR framework for the bank of Sri Lanka respectively. Although the bank framework is more related, the technology gap, culture and context of the organization, the human aspect, and the knowledge gap, and the type of risk and nature of disaster are far different from our country's perspective.

Shropshire&Kadlec (2009) and Hoong and Marthandan (2014) used a quantitative method to develop ITDRP construct and critical dimension of ITDRP respectively. Even though the culture and context, and other factors discussed above hold true, the first one conducted on post-

application of DRP and does not consider pre-application of DRP. The second one is conducted only in financial sectors and does not consider other sectors. Prematha (2017) conducted a component-based ITDRP framework and used design science methodology. The factors discussed above also hold true for this study. This study is very crucial to consider in the future as it is flexible, scalable, and modular as it supports multi-vendor outsourcing, multi-vendor cloud, and multi IT solutions. This technological practice is not in place in our context and it is brought here to be considered in the future by other researchers when we reach out to such technology and time and technology allows.

2.16. Conceptual Framework

A conceptual framework is a network, or "a plane," of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena. The concepts that constitute a conceptual framework support one another, articulate their respective phenomena, and establish a framework-specific philosophy (Yosef, 2008). The goal of a conceptual framework is to categorize and describe concepts relevant to the study and map relationships among them. (TONETTE and MARIA, 2009). The ITDRP framework for Banks of Ethiopia aims to gather all relevant ITDRP steps in one view. The steps and concepts are drawn from the literature. The Framework clearly shows the sequences of the steps, the dependencies between the different steps, and the overall process in a consolidated way. There is a clear requirement to build a conceptual framework essential for recognizing IT DRP for Banks of Ethiopia. The vital aim of the IT DRP for Banks is to build, review and document a reasoned and easily comprehensible plan which will aid the Banks in recovering swiftly and efficiently from the unanticipated emergencies which act as a deterrent to the functioning and operations of the Bank. It also enumerates the role, process and the list of requirements that shall be utilized to organize and regulate the circumstances after a disaster has occurred. The fact on the ground is that Ethiopian banks should consider the international standards while developing ITDRP document. However, adopting an existing international standard would not be feasible since there are difference in organizational culture, technology difference, and other factors.

2.16.1. Framework Components and Explanation

The conceptual framework consists of three main parts. The first is pre-phase plan. It consists of project initiation and IT business service analysis. The second phase is plan phase which is strategy development and writing the plan. This phase depends on the development of the first phase and cannot be developed without it. The third one is post-plan phase. It includes ATTE (Awareness, Train, Test and Exercise) and MA (Maintenance and Audit). This phase depends on the first two phases which should be developed first and foremost.

The following list of themes were identified from the pieces of literature and interview questions were devised and prepared accordingly.

- **Project Initiation:** Businesses must establish the need for disaster planning and define a project plan to guide development efforts. The major tasks included in the initiation stage are: securing management support, organizing the planning project team, establishing the project management process, obtaining the required resources, and developing initial project objectives (Luckey, 2009).
- **IT Business and Service Analysis:** A series of assessments to identify the core IT business scenarios, IT business impacts, potential IT threats and risks, inventory of all IT systems and associated services, and resources deployed to support them. It consists of **IT Inventory**, **IT Risk Assessment** and **IT impact analysis** (Kadlec and Shropshire, 2009; Somasekaram, 2017).

  IT Inventory: Based on the business inventories, identify IT inventories, such as systems, applications, hardware, data connectivity, utilities, and infrastructure services. (Somasekaram, 2017; Acronis, 2016; Susan, 2007)

  IT Risk Assessment: Risk analysis on IT inventory from a disaster recovery viewpoint, performed to identify critical technical components, such as servers and storage and the risks associated with them, and the subsequent impact and probability so that mitigations can be developed. (Somasekaram, 2017; Acronis, 2016; Susan, 2007)

  IT Impact Analysis: The business impact analysis plays a significant role in the identification of the risks associated with the business elements, while it also helps to define the business requirements in a quantifiable way in the form of a maximum tolerable downtime, recovery point objective and recovery time objective. (Somasekaram, 2017; Acronis, 2016; Susan, 2007).

Maximum Tolerable Downtime: It defines the total downtime that a business can accept. MTD is always greater than or equal to RTO. (Brotherton and Dietz, 2014; Somasekaram, 2017).

Recovery Point Objective: Indicates the amount of data loss that can be accepted when a crisis occurs. (BS ISO 22301:2012; Somasekaram, 2017).

Recovery Time Objective: The total time that is required to recover an IT solution after failure. (BS ISO 22301:2012; Somasekaram, 2017).

- **Develop IT Recovery Strategies:** Define and specify the approaches, policies, procedures, and processes to implement the needed resilience to achieve the principles of incident prevention, detection, response, recovery, and restoration. The pre-disaster, during disaster and post-disaster phases of recovery strategies are defined here. It includes Human aspect and responsibilities, IT DR action plan strategies and IT DRP strategy testing, and evaluating strategies.

  Human Aspect Strategies: The teams needed to move the operations to the DR Backup Site and the Emergency Operations as well as their responsibilities. (Somasekaram, 2017; Acronis, 2016; Susan, 2007; Hossam, 2014; Kadlec and Shropshire, 2009; Hossam, 2014; NIST 800-34).

  IT DRP Strategies: To recover critical business functions, restoration of the critical Applications and critical network connectivity is the prioritization plan of the business critical functions. (Somasekaram, 2017; Acronis, 2016; Susan, 2007; Hossam, 2014; Kadlec and Shropshire, 2009; Hossam, 2014; NIST 800-34).

  Testing and Evaluating Strategies: Evaluating and testing strategies to return data processing activities to the primary facilities or another computer facility. (Somasekaram, 2017; Acronis, 2016; Susan, 2007; Hossam, 2014; Kadlec and Shropshire, 2009; Hossam, 2014; NIST 800-34).

- **Develop an ITDRP Plan:** Based on the information and steps listed above, identify and prepare an ITDRP documentation of specific policies and procedures to be used in the event of a disaster (Hossam, 2014; Acronis, 2016; Susan, 2007; BS ISO 22301:2012; NIST 800-34).
- **Conduct Test, Exercise, awareness, and training:** Give bi-annual awareness and training once the plan has been developed. Overall testing should also be conducted per annum or

quarterly as needed by the bank. Exercising after the new training and awareness is mandatory and recommended by pieces of literature (Hossam, 2014; Acronis, 2016; Susan, 2007; BS ISO 22301:2012; NIST 800-34)

- **Conduct Disaster Recovery Plan maintenance and Audit:** Changes are inevitable, IT DRP requires continuous support and maintenance to fit the current requirements. Auditing the IT DRP documents, the technology, and human aspects are crucial to fit changes and preparedness (Hossam, 2014; Acronis, 2016; Susan, 2007; BS ISO 22301:2012; NIST 800-34).

The conceptual framework developed from themes identified from literature and as stated above is visualized in the figure 2.5.

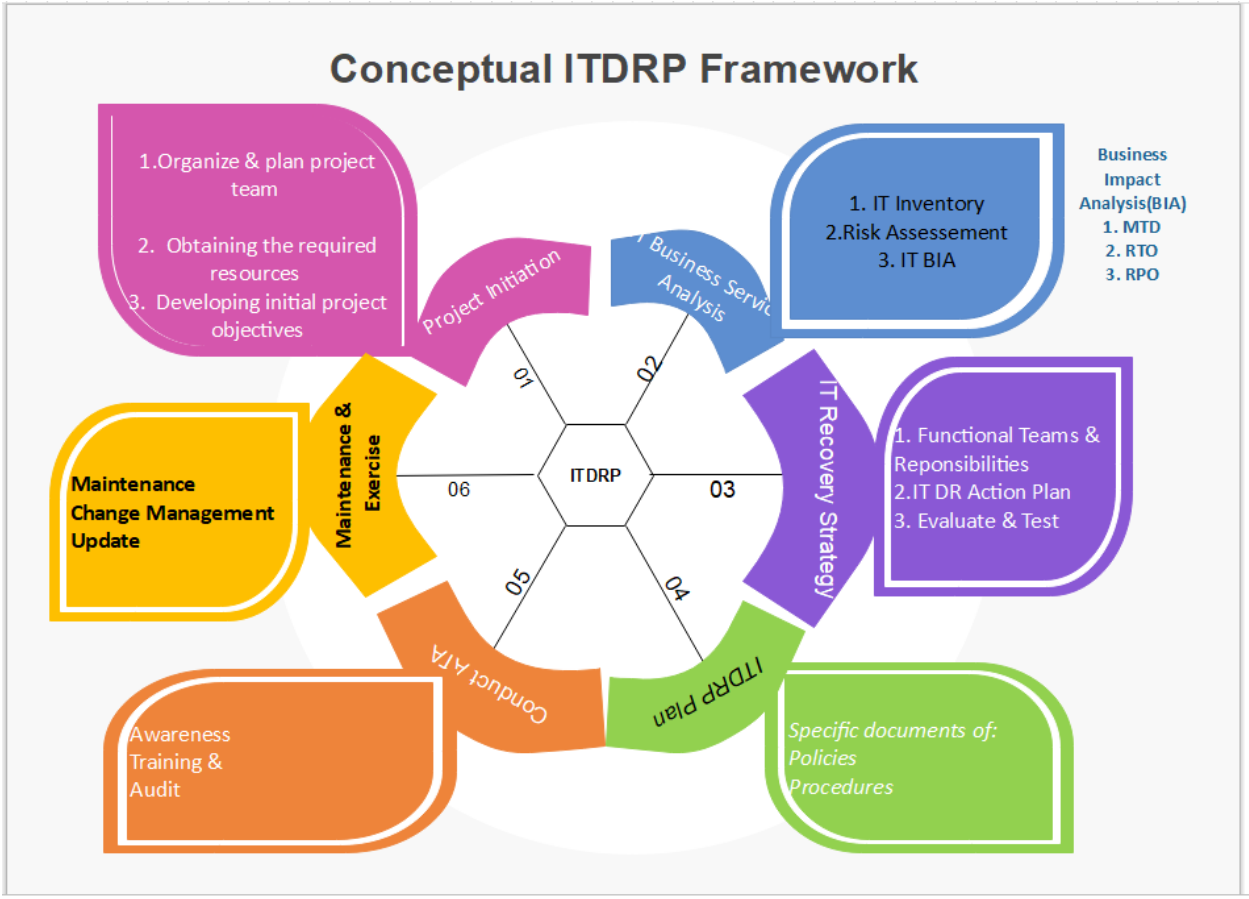


Fig. 2.4. Ethiopian Banks ITDRP Conceptual Framework

The list and description of the steps identified from the literature and its sources are presented in the table. For the details please refer Appendix H in the Appendices section of the document on page 97.

2.17. Chapter Summary

In this chapter, literature relevant to IT disaster recovery is reviewed. Disaster recovery planning elements, process, strategies, techniques, standards, and models are identified to help conceptualize the ITDRP framework. Six ITDRP steps with sub elements have been identified from the literature and, framework is conceptualized. The description of the steps has been presented using a table. Interview protocol has been developed from the conceptual framework and attached as appendix A. Business Continuity plans should be synchronized with ITDRP. Its success in turn requires handling the human aspects and allocating necessary resources to attain the overall objective of IT disaster recovery preparedness.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1. Introduction

The research process is systematic in that defining the objective, managing the data, and communicating the findings occur within established frameworks and in accordance with existing guidelines (Carrie, 2007). The frameworks and guidelines provide researchers with an indication of what to include in the research, how to perform the research, and what types of inferences are probably based on the data collected. Research questions help researchers to focus thoughts, manage efforts, and choose the appropriate approach, or perspective from which to make sense of each phenomenon of interest (Williams, et.al. 2005). The purpose of this chapter is to design appropriate research methodologies that are used to carry out the study in line with the research objectives and research questions. This chapter discusses the research design and methodology, approaches, strategy, study setting, case selection, study participants, data collection instruments, validity and reliability of the study to be tested by domain experts. The chapter also discusses the procedures to be followed when conducting the research to develop a proposed framework for banks of Ethiopia.

3.2. Research Design

A research methodology is a systematic approach to study a research problem from the theoretical underpinning of the research to the collection, analysis, and interpretation of the data (Kothari 2007). It guides the research towards achieving its objectives (Creswell et al. 2003). The research methodology includes a variety of research methods that can be used for collecting, analyzing, and interpreting the data, and determining which specific research methods are appropriate and how these methods can be used for adequately answering the research questions (Creswell et al. 2003). Selecting an appropriate research methodology in a research project greatly depends on the nature of the research.

3.2.1. Research Approach

The research approach is an inquiry strategy that revolves around the underlying assumptions based on which the research design, as well as data collection, is developed (Myers, 2009). As per the most known classification, there are mainly two approaches to research: quantitative and qualitative. While at one level, these two approaches differ based on the knowledge nature; on the other level, they are distinguished by the way to collect and analyze the data leading to data. The three common approaches to conduct research are quantitative, qualitative, and mixed methods (Williams, 2005). The researcher anticipates the type of data needed to respond to the research question. For instance, it is numerical, textural, or both numerical and textural data needed. Based on this assessment, the researcher selects one of the three aforementioned approaches to conduct the research. Researchers typically select the quantitative approach to respond to research questions requiring numerical data, the qualitative approach for research questions requiring textural data, and the mixed methods approach for research questions requiring both numerical and textural data.

3.2.1.1. Qualitative

Qualitative research is the approach for exploration as well as grasping the meaning which groups and individuals assigned to a social or human problem (Creswell, 2013). In qualitative research, the emphasis is on the collected words followed by an analysis of the data (Bryman and Bell, 2007). The approach adopted is an inductive approach in qualitative research wherein the outcome of the research is a description of the general properties of cases and its explanation. In an inductive approach, the researcher draws inferences from the findings and observations that are generalizable in order to develop a new concept (Bryman and Bell, 2011). Qualitative approaches can make a choice from a number of research strategies such as narrative theory, grounded theory, ethnography and case studies (Saunders et al., 2012). Qualitative research does not usually employ statistical procedures or other means of quantification, focusing instead on understanding the nature of the research problem rather than on the number of observed characteristics. Qualitative researchers generally assume that social reality is a human creation, they interpret and contextualize meanings from people's beliefs and practices (Denzin & Lincoln, 2011). On the other hand quantitative research is driven by investigators with the need to quantify data. What constitutes a quantitative research method involves a numeric or statistical approach

to research design. When objective theories are tested by means of examining the relationships amongst the variables it is termed as quantitative research (Creswell, 2013; Myers, 2009; Bryman and Bell, 2007). When it comes to quantitative research, the best approach to be adopted is the deductive approach wherein the research is guided via the theory (Collis and Hussey, 2014). In the case of a deductive approach, the researcher first studies the theory which helps in the formulation of the research hypothesis. In the next phase, the collection of data takes place and its findings help in either the confirmation or rejection of the hypotheses. Based on this, revisions are carried out within the theory (Bryman and Bell, 2007). According to Collis and Hussey (2014), experimental and survey research strategies are included in quantitative studies. A survey is conducted via means of structured interviews, questionnaires and even structured observation of actions and decisions (Saunders et al., 2012). Mixed research mixes or combines qualitative and quantitative techniques, methods or designs to explore a single research topic. The justification for this approach is that it provides the most authentic findings, that it is most favorable for external validity. Mixed approaches are not based on a fixed paradigm: they include a number of variants and hybrid forms, including mixed models and mixed methods, allowing a flexible approach to data collection and analysis (Arthur 2019). In this study a qualitative approach is used to conduct the research.

3.2.2. Research Strategy

The plan drawn out by the researcher on how to respond to the research questions is termed as the research strategy. It is the methodological association between the philosophy that has been chosen and the methods chosen for the collection and analysis of data (Saunders et al., 2012). When it comes to research strategies, there are a number of them to choose from; survey, experiment, grounded theory, case study, archival research, ethnography and narrative inquiry (Saunders et al., 2012). Quantitative research is associated with surveys and experimental studies (Collis and Hussey, 2014). As mentioned in the earlier sections, the current study has adopted the qualitative approach and therefore the chosen research strategy for the study is the case study.

Case study research involves an intensive study of a single unit for the purpose of understanding a larger class of (similar) units observed at a single point in time or over some delimited period of time (Sasa, 2014). As such, case studies provide an opportunity for the researcher to gain a deep

holistic view of the research problem, and may facilitate describing, understanding and explaining a research problem or situation. The case study enables a researcher to closely examine the data within a specific context. In most cases, a case study method selects a small geographical area or a very limited number of individuals as the subjects of study. Case studies, in their true essence, explore and investigate contemporary real-life phenomena through detailed contextual analysis of a limited number of events or conditions, and their relationships (Zaidah, 2007). The case study research can be designed as either single or multiple cases (Yin, 2009). In this case Ethiopian Banks are selected as a study setting. A single case is often selected if the case under study is both an exemplary case containing extreme and/or unique circumstances (Yin, 2009).

3.2.2.1. Framework Development Procedure

Research framework development procedure is the overall plan or steps to follow to develop the proposed framework for the study.

This study follows the following procedures to conduct the research.

1. Conducting a literature review to capture IT DRP concepts
2. Conceptualize IT DRP in a framework
3. Assessing the current DRP practice and challenges of the selected private and government Banks in Ethiopia based on the conceptualized IT DRP framework
4. Analyze collected data and discuss the findings in the context of DRP concepts from the Literature, existing DRP standards and models.
5. Get the framework evaluated by domain experts for its feasibility.
6. Incorporate the experts' feedback if any to update the proposed IT DRP framework.
7. Concluding the study with a summary of the findings, the updated framework, and recommendations.

3.2.3. Study Setting

Banks are selected as a study setting.

The following table shows government-owned banks and selected private banks.

No	Bank Name	Private or Government	Remarks
1	Government owned Bank of Ethiopia	Government	Bank A
2	Private owned Bank of Ethiopia	Private	Bank B

Table 3.1. List of Government and Private Banks

3.2.4. Case Selection

Case selection in case study research has the same twin objectives as random sampling; that is, one desires (1) a representative sample and (2) useful variation on the dimensions of theoretical interest. One's choice of cases is therefore driven by the way a case is situated along these dimensions within the population of interest (John, 2008). As sampling is a process of selecting a representative fraction of the population, a purposive sampling is employed to select targeted IT directors, top-level business managers, and contingency or risk management departments of the banks. Simple random sampling is used to represent a government owned bank and a Private owned Bank. Random sampling will be used as it is a probability sampling method. In random sampling, each member of the population has an equal chance of being selected. The sampling scope refers to a list or set of directions that identifies the target population. Thus, the target population of this study is the employees of government-owned and private banks in Addis Ababa.

3.2.5. Study Participants

The participants for this study will be Commercial Banks of Ethiopia's, and Awash International private banks' IT Audit directors, IT Security Directors, risk managers, IT Data Center managers, CIOs, IT security Managers, and incident teams and managers who are located at Addis Ababa city head offices of the two banks.

3.3. Research Techniques

In this study interview is used to conduct the research. Interviews are a systematic way of talking and listening to people and are another way to collect data from individuals through conversations. Interviews as an interchange of views between two or more people on a topic of mutual interest, sees the centrality of human interaction for knowledge production, and emphasizes the social situatedness of research data. Interviews are ways for participants to get involved and talk about their views. In addition, the interviewees are able to discuss their perception and interpretation in regard to a given situation. It is their expression from their point of view. Interview is not simply concerned with collecting data about life: it is part of life itself. Its human embeddedness is inescapable. There are many reasons to use interviews for collecting data and using it as a research instrument. Gray (2004) has given the following reasons: there is a need to attain highly personalized data, there are opportunities required for probing, a good return rate is important, and respondents are not fluent in the native language of the country, or where they have difficulties with written language. Also, the interview needs to be effective and this is the responsibility of the researcher. The researcher ought to have the following skills and abilities: An ability to listen; an ability to be non-judgmental; a good memory; ability to think on his/her feet. An interview guide is also an essential component for conducting interviews. An interview guide is the list of questions, topics, and issues that the researcher wants to cover during the interview. The interview guide should be clear and avoid ambiguity (Kajornboon, 2005; Cohen, et al, 2000; Gray, 2004; Koskei and Simiyu, 2014*)*

In this study an interview guided by interview questions drawn from major areas of framework concepts are used to conduct the interview.

3.3.1. Data collection

Data collection is the process of gathering the desirable information carefully, with least possible distortion, so that the analysis may provide answers that are credible and stand to logic (Sapsford & Jupp, 2006). Data type can be primary or secondary. The data gathered by researchers' first-hand is primary data. The researcher collects such data on purpose, because no previous records of the data exist to be accessed by the public. Primary data can be collected using a range of methods like surveys, interviews, focus groups, etc. Such data is considered to be highly reliable. The data that have been collected and compiled by someone, and are accessible to the public, are known as secondary data. It is the data used by the investigator from previous studies and other sources. The primary data collected for one research study, becomes secondary data when it is further used for another research. Generally, secondary data includes government reports, census data, departmental records, etc. Using such data is less expensive and faster in comparison to primary data. In this study the primary data will be collected through an interview.

3.3.2. Data Analysis Strategy

It is not possible to describe set procedures that can be applied in a fixed sequence in all qualitative analysis. As a result, it is necessary to focus initially on principles of analysis and resulting guidelines, rather than fixed techniques. The most common kind of analysis of qualitative data is thematic analysis. It is concerned with the identification and analysis of patterns of meaning (themes) and constitutes a widely applicable, cost-effective and flexible tool for exploratory research. Thematic analysis is particularly suitable for analysing experiences, perceptions and understandings. It can be used to analyse a large variety of qualitative data and is a flexible method which can be applied within various theoretical frameworks. Thematic analysis is also applicable independently of any initial theory and can be used for purely inductive research. Furthermore, it is suitable for the analysis of small, medium-sized and even large data sets. (Braun and Clarke, 2013).

Thematic Analysis is considered the most appropriate for any study that seeks to discover using interpretations. It provides a systematic element to data analysis. It allows the researcher to associate an analysis of the frequency of a theme with one of the whole content. This will confer accuracy and intricacy and enhance the research's whole meaning. Qualitative research requires

understanding and collecting diverse aspects and data. Thematic Analysis gives an opportunity to understand the potential of any issue more widely (Marks and Yardley, 2004). Qualitative research needs to be able to draw interpretations and be consistent with the data that is collected. The participants' interpretations are significant in terms of giving the most appropriate explanations for their behaviours, actions and thoughts. This fits in well with the features that are involved in the process of Thematic Analysis (Creswell, 2003). In this study thematic analysis is used to interpret the themes from the interview of participant's audio records against the identified concepts in the conceptual framework. The research results are interpreted from the qualitative perspective of the research process that can generate effective outputs.

3.3.3. Validity and Reliability

Validity in research is concerned with the accuracy and truthfulness of scientific findings. A valid study should demonstrate what actually exists and a valid instrument or measure should actually measure what it is supposed to measure. There is Internal and external Validity in qualitative research. Internal validity refers to the extent to which research findings are a true reflection or representation of reality rather than being the effects of extraneous variables. External validity addresses the degree or extent to which such representations or reflections of reality are legitimately applicable across groups.

Reliability is concerned with the consistency, stability and repeatability of the informant's accounts as well as the investigators' ability to collect and record information accurately. It requires that a researcher using the same or comparable methods obtain the same or comparable results every time he uses the methods on the same or comparable subjects. One of the key factors affecting validity and reliability is error. Error is inherent in all investigations and is inversely related to validity and reliability. The major sources of error can be the researcher, the subjects participating in the project, the situation or social context and the methods of data collection and analysis. The major critical strategies essential for producing trustworthy and believable findings in qualitative research are triangulation, multiple repetitions of measurement, expert consensual validation from others familiar with the topic, member check, searching for disconfirming evidence, checking for representativeness, and thick description. To develop a valid, truthful and believable account of qualitative studies it will be wise to take note of and implement those critical

strategies. From those strategies, expert validation is implemented in this study (Kimberlin and Winterstein, 2008; Nahid, 2003; Ali, 2011).

3.4. Chapter Summary

The chapter aim was to clearly outline the research design of the thesis. Thus, for the purpose of this study, the qualitative approach for conducting research was adopted since the main focus of the study is to develop and create a proposed framework for IT DRP for Banks of Ethiopia. After that, the chapter made clear distinctions between the various research approaches and zeroed in on the qualitative approach rather than the quantitative approach. Qualitative research helps in making use of a number of data collection methods, the participant's meanings and the relationships are studied for the development of a new theory.

Thereafter, the chapter focuses on the different research strategies and found out the case study strategy that would be used for the present research. The steps and procedures to develop the proposed framework are outlined to be followed. Furthermore, the chapter talks in detail about the research techniques, data collection methods, study setting and case selection. This chapter has also discussed the validity and reliability strategies that are used in qualitative research approaches.

CHAPTER FOUR: DATA PRESENTATION ANALYSIS AND DISCUSSION

4.1. INTRODUCTION

This chapter presents the data obtained from interviews of one government and one private bank. The interview is conducted as a face-to-face interview and using the phone. Both cases are presented based on the IT DRP areas identified in section 2.16. Discussions and current challenges of the Banks are also presented.

4.2. PARTICIPANT AND ORGANIZATIONAL INFORMATION

The study participants in both cases were Chief Information officers, IT Audit directors, Risk assessment managers, IT security directors, IT security managers, newly established IT business continuity and disaster recovery managers (only one case), Data Center managers, and Infrastructure and application managers. The researcher also used phone interviews due to the inconvenient office time for some Chief Information Officer and Data Center manager.

Bank A is organized in such a way that there is a chief information officer under which there exist five departments. The departments are Information System (IS) security, IS quality assurance, Information systems, IS program management, and IS service strategy management. Under the vice president of Information Systems, business continuity and disaster recovery section is newly established. The business continuity and disaster recovery section is the one in charge of the IT DRP development. The Information systems department also includes application management, infrastructure management, information management, IS operation support, and system development, integration and customization sections. For the details of the structure please refer to Appendix C on page 82.

Bank B has also chief information officer under which IT security division, Infrastructure and service management division and IT business solution division are structured. The IT security division is in charge of all the security issues. Each division has sub units which are established to satisfy the different needs of the bank B.

4.3. CHALLENGES IN DATA COLLECTION PROCESS

Initially it was planned to conduct interviews on three banks to represent government owned banks and private banks. Unfortunately, the second and new era private bank denied to accept the research and interview. After a letter of assistance and cooperation was received from AAU on the beginning of February 2020, the first letter was submitted to Buna Bank. The HR of the bank refused to accept the letter. They explained an agreement was made among bank executives not to receive any research letter. I tried to explain the importance of the study for the bank and HRO advised me to contact the executive director. The director was out of office for a meeting for a week and I had to make a bunch of calls to reach the secretary. She told me the letter was forwarded back to HR and I contacted the HR again. After multiple times of phone call, the answer was no and the denial came true.

The second letter was also denied by HR in the same way. But after multiple trials and thanks to the CIO, the IT department was willing to accept the letter and managed to conduct an interview. The third letter was submitted to another government bank. This bank has a moderate way of managing research. It has a learning and development department which receives and writes internal memos to the concerned department. They do not receive "To Whom It May Concern" letter and I had to come back to AAU to have the department re-write the letter directly to the Bank. After the corrected letter, I signed an agreement with the bank to keep confidential data secret and provide one copy of the product to the bank at the end of the day. Another challenge here wass to be urged to make phone interviews with some managers. They were busy during office hours and interviews had to be made at their convenient time. The study aimed to involve the banks' IT Audit directors, IT Security Directors, risk managers, IT Data Center managers, IT Security Directors, IT security Managers, and incident teams and managers. Unfortunately both Bank's incident team's managers were not available during the data collection. But the interview with IT BC and DR Manager of bank A and Infrastructure and application manager of Bank B were unplanned and awesome.

4.4. DATA PRESENTATION

4.4.1. DATA FROM INTERVIEW

The interview involved asking questions, listening to, taking notes and recording answers from an individual and group in a structured and semi-structured format in an in-depth manner. The interview question was written in English and the answers were in Amharic. A translation of language and transcription of the recording was made to present the data.

The concepts are drawn from the conceptual framework. It has three phases. 1.) Pre-plan phase includes project initiation and IT business analysis. The IT business analysis consists of IT inventory, IT risk assessment and IT business impact analysis such as RTO and RPO. 2.) Plan phase includes the recovery strategies and developing the actual IT DRP document. 3.) Post-plan phase includes the testing, training, awareness and exercise as well as the maintenance and ITDRP audit. In the following interview was made with interviewees per each area as a process that has been included in the framework. The briefing has been made to the interview about each area which becomes the process or steps to follow in the course of developing the ITDRP document.

Project Initiation

An interview question was raised to explain in what circumstances the IT disaster recovery plan has been initiated in bank A. The business continuity and IT DRP manager explained:

"This section is under development and newly established. The IT security directorate used to manage it. Due course attention was not given and IT DRP was overseen by the bank. But recently the bank learned its importance and established a business continuity and disaster recovery section that initiated the project. The project can be initiated in two ways. The first one is using a consultant agency from an external organ and the second is by the Bank's internal staff. In our case the project was initiated by internal staff. A gap analysis was made using the ISO/IEC 22301 by Bank's internal teams".

The IT audit director added *"we are forcing the section to develop a standardized IT DRP plan and the report is submitted to the board of directors. We also necessitate it by checking against*

regulatory bodies like the national bank of Ethiopia. So that management was involved in the initiation of the IT DRP and approved it".

Bank B's Infrastructure and service management division head said;

"The IT DRP plan was initiated by the bank's business team which includes IT teams and regulatory bodies. After approval of the project it follows a project lifecycle as usual. IT DRP is incident driven and it was overlooked by management as priority was given to core business needs. The business continuity and disaster recovery section was not established yet. But the development is under initiation and we did not decide which standard to follow". The Data center supervisor of Bank B explained *"The role of management is high as there is enforcement from internal business units and external regulatory bodies like the national bank of Ethiopia".*

IT Inventory

The IT audit director and IT infrastructure manager of Bank A both said

"We are doing IT inventory as part of asset management".

The Business continuity and disaster recovery manager of Bank A described *"ITIL process is implemented to facilitate the process and IT asset management is automated. So that asset management software is used to control the IT inventory system of the bank".* He added "*confidential items, equipment, applications, software, tools, systems, etc. are well identified as part of IT inventory in particular and IT DRP in general".* The information security manager of Bank A highlighted *"sensitive and expensive security devices, equipment and systems are identified and managed as part of IT inventory".*

The Infrastructure service management division head and data center manager of Bank B said *"application, system, hardware, software, equipment, tools and services of data center and other inventory is done using excel spreadsheet. We have no specialized database to manage and control inventory. We recently established a service management unit and delivery team to identify services, critical systems, etc. and rank as well as prioritize them according to our criticality as high, medium or low".*

They also explained the asset management is under development and not in its full or mature functionality.

IT Risk Assessment

Bank B's CIO and Infrastructure service management division head said

"Any risk is assessed by the combination of Bank's IT audit team, risk and compliance management team, security team, risk identification and assessment team. Enterprise level risk management is not in place. There is a formation of a potential unified risk assessment team establishment underway but not in a good maturity level. There is a capability gap towards the establishment of enterprise level unified risk management. But the IT risk identification and assessment is working 24/7. After risks are identified, it will be reported to management and board directors and a mitigation action is taken to resolve the incident. A formal risk analysis is done in each section of the bank separately".

Bank A's Risk manager suggested that they are not doing IT risk assessment and analysis and recommended to contact the IT security section. The IT security manager of Bank A said *"We are conducting a formal IT risk assessment and analysis per the regulatory body and internal audit advises and bank's international standards"*. Bank A's IT audit director and Infrastructure manager said *"we work with the risk and compliance section of the bank and ensure risk assessment lifecycle is followed and in line with the business strategy as well as regulatory body and risk governance"*. The IT audit director added

"We also follow two approaches to identify risks. Those are risk based audits which allow us to identify risks with high, medium and low impact and report to management and board directors. The second one is to follow a risk assessment lifecycle. The risk analysis is done per the standards and recommend and advise the bank to follow standards whenever we assess IT related risks".

IT Business Impact Analysis

The Infrastructure service management division head and Data center supervisor of Bank B underlined *"Because of the limitation of telecom infrastructure the business impact analysis was*

not done according to the standards. But we had made support and maintenance services and have premium agreements for the critical system. Recovery point objective and recovery time objective is not set in our bank".

The business continuity and disaster recovery manager of Bank A stated

"We have not made business impact assessment. We believe we are in the project initiation phase and on the IT inventory step. We will follow the step and assess outage toleration, resource identification and mapping, dependencies of systems and others will be identified per ISO standards".

Recovery Strategies

The business continuity and disaster recovery manager of Bank A explained

"The recovery strategies are not well organized. There are separate general policies and procedures for tape based traditional backup and recovery strategies. They are not done according to the standard. Services plan has also taken longer time. The hot site is in place but the full documentation, policies and strategies are not in place". The data center manager said *"we are taking tape backups. We are taking full backup once and use incremental backup afterwards. We were able to restore from technical and software crashes and it was one part of a test that the bank can restore from a crash in this scenario. But in case of catastrophic scenarios where restoration from relocation is necessary, it will be difficult".*

The Infrastructure service management division head and Data center supervisor of Bank B explained

"There are generic policies and procedures developed by the infrastructure team since there is no isolated disaster recovery team established. The damage assessment is made by the same team. There is no specific document about strategies. There is no regular test needed as there is no hot or warm site. But basic facilities and human elements are in place on the cold site. First respondent and supervisors are in place. We also have a power surge, cooling system, redundant infrastructure and cable systems on the site".

Disaster Recovery Plan

The Infrastructure service management division head and Data center supervisor of Bank B said, *"There is no IT disaster recovery plan document in place. The information technology disaster recovery plan is under development by selected IT teams. It is in the initiation stage. We are trying to follow the international standards like ISO, COBIT, ITIL and NIST but unable to confirm which standard fits our bank. So we were urged to train the IT staff. Four of the IT staff have been selected to take the train and it was no use more than giving awareness. Lack of BC and DR division or lack of a focused team affected the Bank to lag behind in developing disaster recovery plans".*

The business continuity and disaster recovery of Bank A's manager said,

"There is no IT disaster recovery plan in place. The newly established BC and DR section is in its emerging stage to develop the document. We are following the ISO/IEC 22301. No one is trained on this document and it is difficult to understand and implement per our bank's context. So that we are seeking for professional certified implementation company to train the staff to help them forward towards the document development and implementation stage".

Awareness, Train and Test

Business continuity and disaster recovery division manager of Bank A said,

"Awareness, training and exercising the IT disaster recovery cannot be dreamed without developing the document. The previous steps should be followed consciously and carefully, the strategies should be developed, specific backup and recovery policies should be developed and tested first. The recovery test approach will be followed after we are able to develop the disaster recovery document".

Bank B's Infrastructure service management division head and Data center supervisor believed *"The document should be developed primarily, at least warm or hot sites should be in place and awareness, training and exercise will follow".*

Maintenance and Audit

The Infrastructure service management division head and Data center supervisor of Bank B suggested,

"The only maintenance we have in place is application and hardware based support and maintenance service with external vendors. We also have 24/7 premium maintenance and support service for critical services and systems. There is no maintenance or update done on IT DRP as there is no document in its full form. We have been advised by internal IT audit and regulatory bodies like the national bank of Ethiopia to develop an IT DRP plan and it is in progress by IT teams".

The IT audit director of Bank A explained,

"We identified the necessity of developing IT DRP plan document per the regulatory advice and enforcement. But there were not focused groups to do so. Recently, per the advice and recommendation, the BC and DR section is established to do the job. We will continue the follow up and report the progress to the management board director as part of our responsibility".

4.5. DISCUSSION

The purpose of the study was to answer the question "how can an IT disaster recovery plan framework be developed for Ethiopian banks?" and to propose a framework for Ethiopian Banks that can be used as a base or quality tool for developing their respective disaster recovery plan according to their business needs. The interview questions based on the concepts and steps derived from the literature were presented in the sections above. The themes will be discussed in the section below in comparison with how the two banks currently perform IT DRP as they have been interviewed and in integration with the literature.

4.5.1. HOW BANK A AND BANK B PERFORM IT DRP

In this section, the discussion based on interviews of the two case studies of Bank A and Bank B from the previous section integrated with the literature are discussed. Literature revealed that without conducting an effective project initiation process, an IT DRP strategy will be incomplete and potentially unsuccessful when activated. For example, an IT professional who attempts to develop a DR plan without engaging other subject matter experts and managers will not be able to accurately assess the time-critical systems or the needs of each relevant stakeholder (Snedaker, 2013). Both Bank A and Bank B tried to prepare a disaster recovery document without project initiation and were not successful. Infrastructure service management division head of Bank B stated that they had a pseudo IT disaster recovery document which they used to show the regulatory bodies. Later they found that it was incomplete and decided to initiate an IT DRP project from scratch. The base for this is after the Bank managers took BC and DRP training by Ethio telecom DRP pre-plan trainers as they explained to me.

In the IT DRP project initiation phase, system requirements are identified and matched to their related operational processes, and initial contingency requirements may become apparent. Very high system availability requirements may indicate that redundant, real-time mirroring at an alternate site and fail-over capabilities should be built into the system design. Similarly, if the system is intended to operate in unusual conditions, such as in a mobile application or an inaccessible location, the design may need to include additional features, such as remote diagnostic or self-healing capabilities. During this phase, the IT system also should be evaluated against all other existing and planned IT systems to determine its appropriate recovery priority. This priority will be used for developing the sequence for recovering multiple IT systems (John and James, 2005). The business continuity and disaster recovery manager of Bank-A confirmed, they are in the project initiation phase and have been identified critical systems but have not ranked them accordingly as they need to do BIA first.

A Business Impact Analysis (BIA) aims to determine which resources warrant the expense and effort of distinct inclusion in a disaster recovery plan. A BIA further specifies the priority by which each time-critical system is recovered after a disaster. The close examination of technology and business processes necessitated by a BIA can also identify potential changes that will reduce

system interruptions or improve service quality. An assessment of current literature indicates that the creation of a BIA is a best practice that should play a central role in DR planning activities. A recent survey of business continuity managers reveals that 20 percent of businesses with continuity plans do not have a current BIA on file, and one third of those companies with a BIA have failed to keep it up to date (Gregory, 2013; Bradbury, 2008). Accordingly, the business continuity and disaster recovery manager of Bank A and Infrastructure service management division head of Bank B stated that they have not developed BIA such as recovery point objective and recovery time objective reasoning telecommunication infrastructure limitation as a challenge.

The literature and international standards proved that the first step in the prioritization process is to define a maximum tolerable downtime (MTD) for each time-critical IT system that specifies how long the business can function after the system fails. The business should also calculate a recovery time objective (RTO) that declares how quickly the system should be restored. The RTO must be less than the MTD to account for delays in the resumption of work after a system outage. The final step in the prioritization process is to create a recovery point objective (RPO) that identifies the amount of information that a business can afford to lose permanently from each system during a disaster. The RPO will determine how frequently electronic data must be backed up to an offsite location from which it can subsequently be restored after a disaster has taken place (Bradbury, 2008; Gregory, 2013; Snedaker, 2013).

Per the conversation with Bank A and Bank B's CIO and business continuity and DR Manager respectively, customer and business requirements are identified, external dependencies (i.e., government, industry, and legal) are identified, a business risk assessment is underway, management support is obtained and project planning is initiated. They explained they will follow the standards like ISO (Bank A) to prioritize the process.

DR planners should also meet with key members of the company, such as those responsible for facility management, to analyze the potential risks with which the company is faced. Such risks could include concerns ranging from a fire or flood in an IT server room to a major earthquake or hurricane that destroys entire facilities. Secondary effects of disasters such as utility and communication outages, should also be considered as potential risks. A formal approach that organizations can follow to identify and prioritize the risks that could lead to a disaster includes: (1) identify each potential disaster that could affect time-critical IT systems; (2) assign a value

between 1 and 10,000 that represents the likelihood of each disaster, with 1 being the least likely to occur; (3) for each disaster identified, rate the potential impact on the time-critical IT systems, again using a scale of 1 to 10,000; (4) multiply the likelihood values by those estimated for the impact; and (5) sort the results to list the risks with the highest calculated numbers, representing the most significant risk, first. The broad range of values allows companies to distinguish clear priorities between many potential risks (Sneaker, 2013; Gregory, 2013).

The IT Audit director of Bank A confirmed that they follow formal risk assessment and audit based risk assessment approach in assessing the risk in the Bank. This complements what the literature stated above.

Recovery activities can be conducted in three approaches. The first one is to move operations to the Disaster Recovery Backup Site and the Emergency Operations Center. This activity will begin with activation of the Disaster Recovery Plan. The second one is to recover critical business functions, restoration of the critical applications and critical network connectivity. The goal here is to recover the systems and network so that the customers can continue business. The third one is to return data processing activities to the primary facilities or another computer facility (Bryan, 2019). In Bank A and Bank B only vendor based recovery activities and strategies are in place.

To adequately respond to a disaster, a business must have a "well thought-out, documented" DR plan in place. IT DR planning best practices indicates that it is during the IT DRP development stage that organizations specify (a) how to react to disaster scenarios, (b) when to activate a DR plan, (c) how each critical IT system should be recovered, and (d) who should perform needed recovery tasks. The key elements identified within this section can guide DR planners as they develop and document IT recovery strategies based on information identified through the BIA process (Spencer & Johnston, 2003). It was well justified by both bank's IT managers that they do not have IT DRP documents in place.

Although no specific law states that a business must have a DRP, there is a body of legal precedent that has been used to hold companies and even individuals responsible for the recovery of data after a disaster (John and James, 2005). According to the business continuity and disaster recovery manager of Bank A, the regulatory bodies like the national bank of Ethiopia necessitates the

development of IT DRP plan. It was also confirmed by the CIO of Bank B that the regulatory body and the internal IT auditors urged the bank to have IT DRP in place.

According to National Institute of Standards and Technology (NIST) Publication SP800-12, the purpose of computer security awareness, training, and education is to enhance security by: Improving awareness of the need to protect system resources; Developing skills and knowledge so computer users can perform their jobs more securely; and Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Awareness stimulates and motivates those being trained to care about security, resources and reminds them of important security practices such as IT disaster recovery. Explaining what will happen to an organization, its mission, its customers, and its employees when security fails or disaster occurs often motivates people to take security more seriously. The success of a disaster recovery effort depends on the effectiveness of the response team. For this reason, all individuals who are assigned a position in an IT DR plan should be included as regular participants in DR testing. It is also important to involve the response team in DR plan testing to give those individuals experiences that enable a "cool and competent" response to a disaster. In addition to training through involvement in recovery testing, other sources such as conference room training and seminar-based instruction should be utilized. If employees are not properly trained to implement a DR plan, the planning efforts will have effectively been "wasted" (Rothstein, 2007; Spencer & Johnston, 2003; Teuten, 2005)

Bank A and Bank B had not conducted post implementation training, awareness and testing since they have no IT DRP in place. But they have conducted some IT DRP awareness for the IT DRP development team who recently initiated the project.

Due to the continuously changing nature of risks that face time-critical IT systems, businesses must ensure that DR plans are updated regularly to reflect the current environment. Depending on the frequency and complexity of changes, maintaining a DR plan "may end up being the biggest challenge" of the DR planning process for some businesses. However, developing an explicit strategy to address DR plan maintenance can reduce the complexity of the task (Teuten, 2005; Snedaker, 2007).

Bank A and Bank B IT managers and CIO confirmed that they have no IT DRP plan to maintain.

4.5.2. **CURRENT CHALLENGES OF BANK A AND B**

The interview participants mentioned various challenges in the course of IT DRP plan development. There were interview questions under each area regarding challenges in Bank A and Bank B. Bank A's BC and DR Manager said the challenge of initiating IT DRP plan was lack of experience, no department and focused group had been in place before the BC and DRP division establishments. Managing and ruling the division to initiate the project had been time consuming. And he also added there was a lack of awareness and training about IT DRP in general.

Infrastructure service management division head and Data center supervisor of Bank B said budget was not an issue in their bank. But since the driving factor of IT DRP is risk or incident, the management used to give priority for other profitable business and there was a lack of urgency or necessitating the management to develop the plan. They also said the management sometimes regard the plan as a luxury business. Those challenging factors lag the establishment of the BC and DR section and they were not able to start the plan in time which is still an issue in the bank. They also said the risk assessment was also a challenge as no separate IT risk assessment and analysis team in place. Regarding the recovery strategy they explained the challenges of having a hot site or warm site in place was challenging because the tele infrastructure link was not guaranteed. They tried a hot site test and only half of the data were replicated and half had been lost and they were urged to cease the service and come back to cold site infrastructure.

They explained the knowledge capacity and gap was also another challenge. Manpower from a market specialized in IT DRP was not found. There were no professional sectors found to be certified in implementing the IT DRP plan in the country and finding them outside the country was also a challenge. Although IT teams were established to initiate the project, there is still a knowledge gap to select and adopt the most appropriate international standard to develop the plan for the bank. To develop the plan with the existing team was time consuming and external consultancy was needed. There were no academic universities and colleges links found in training and implementing IT DRP and BC in the country and they are interested to work with academies to solve such problems and other related issues.

According to the Data center manager of Bank B, there was also a spare part availability challenge regarding the disaster recovery and data center expensive and critical systems. They tried to

diversify the backup and recovery system to overcome the shortcoming of IT DRP but all activities were not documented.

4.6. IT DRP FRAMEWORK VALIDATION

ITDRP framework process or steps should be evaluated through well-executed method to prove the quality and efficiency of developed framework. The variable and measurement criteria used to evaluate the IT DRP framework are functionality, completeness, reliability, usability, and fit to the Bank. Those validation criteria are some of the relevant quality attributes prior to use it to the intended goal. An IT DRP framework are evaluated through expert validation method. These evaluation method can be chosen based on the study that the research is conducted. In this study, expert validation method is used to evaluate the proposed framework. Accordingly, focus group from both banks was used to gain expert validation. The experts from both banks confirmed that this will greatly help them in the process of IT DRP framework development underway. They commented each area should be included and have no point to drop. The expert validation was chosen to gain different views of the business continuity and IT DRP, security directors, security managers, risk managers, and other experts who work in both Bank A and Bank B of Ethiopia in various IT positions. The knowledge of the subject matter of the expertise in IT DRP will help to gain valuable inputs and proper investigation of the proposed IT DRP framework. Besides, the experience of the knowledge area experts in the Banks in different positions also adds value to the holistic view of the proposed Information Technology disaster recovery plan framework.

Validation Comments from experts in Bank A

The Business continuity and disaster recovery division manager of Bank A commented

"We are on the process of developing the IT DRP plan. Management acceptance is secured and we initiated the plan recently. This is nice and helpful as it consists of all the complete areas that we actually go through in the process of developing the plan. The reliability and usability of the areas included in the framework fits to our bank and the steps are valid. We used the IT inventory as part of auditing the general IT software and hardware. But we learned from the framework that IT inventory as part of ITDRP document is useful and fits to our plan document. The inclusive of the recovery strategies to consider each and every process is an essential part that the bank will consider as critical part. In general, all the areas the bank need to include in the plan are included

and complete. I do not find a point to drop in this plan. But I want to comment if implementation is considered".

The Data Center Manager of Bank A Said

"MTD, RPO and RTO included under the business impact analysis are essential parts that over looked by the bank for many years. They are important metrics to be considered as we have only premium service level agreements for our critical applications. The testing, training, awareness, exercise and maintenance process in the framework are crucial usable steps and fits to our plan".

The IT audit director of Bank A commented

"This is what we used to recommend our bank. I like the inclusive of IT Audit as part of the process to help us follow up each and every step to be implemented as per the plan. Our regulatory bodies always force the bank to have IT DRP in place but do not give us the detail or framework to go through. This framework is a good guidance for our bank and new and emerging banks under development in our country. I found it all areas are useful to consider".

Validation Comments from experts in Bank B

After the framework is resent using the expert validation criteria to expert in Bank B, the following are commented. The Infrastructure service management division head and Data center supervisor of Bank B commented;

"The established focused group development teams are on way of developing the plan. We found the framework is inclusive and complete. Our current technology is in line with the areas depicted in the framework diagram. We are following the ISO standards to develop the framework but ISO lacks coverage area and details. We find this framework usable and referable throughout our development of the plan document and no area to drop from the proposed framework. But in the future if we update our technology, we will need to maintain our plan and document".

The framework will be used to ensure consistency of disaster recovery planning practice among Ethiopian Banks. It will increase the efficiency and effectiveness of the services provided by the banks. It can also be extended to other financial sectors with minimum modification and used as a major input to develop IT DRP framework for other organizations in Ethiopia as it is developed in

the context of Ethiopian Bank's culture, technology, understanding, knowledge gap and human elements factor. The final proposed framework is as below. There is no difference between the proposed and final framework as the area expert made no comments to drop any of them or concepts from the previously proposed IT DRP framework.

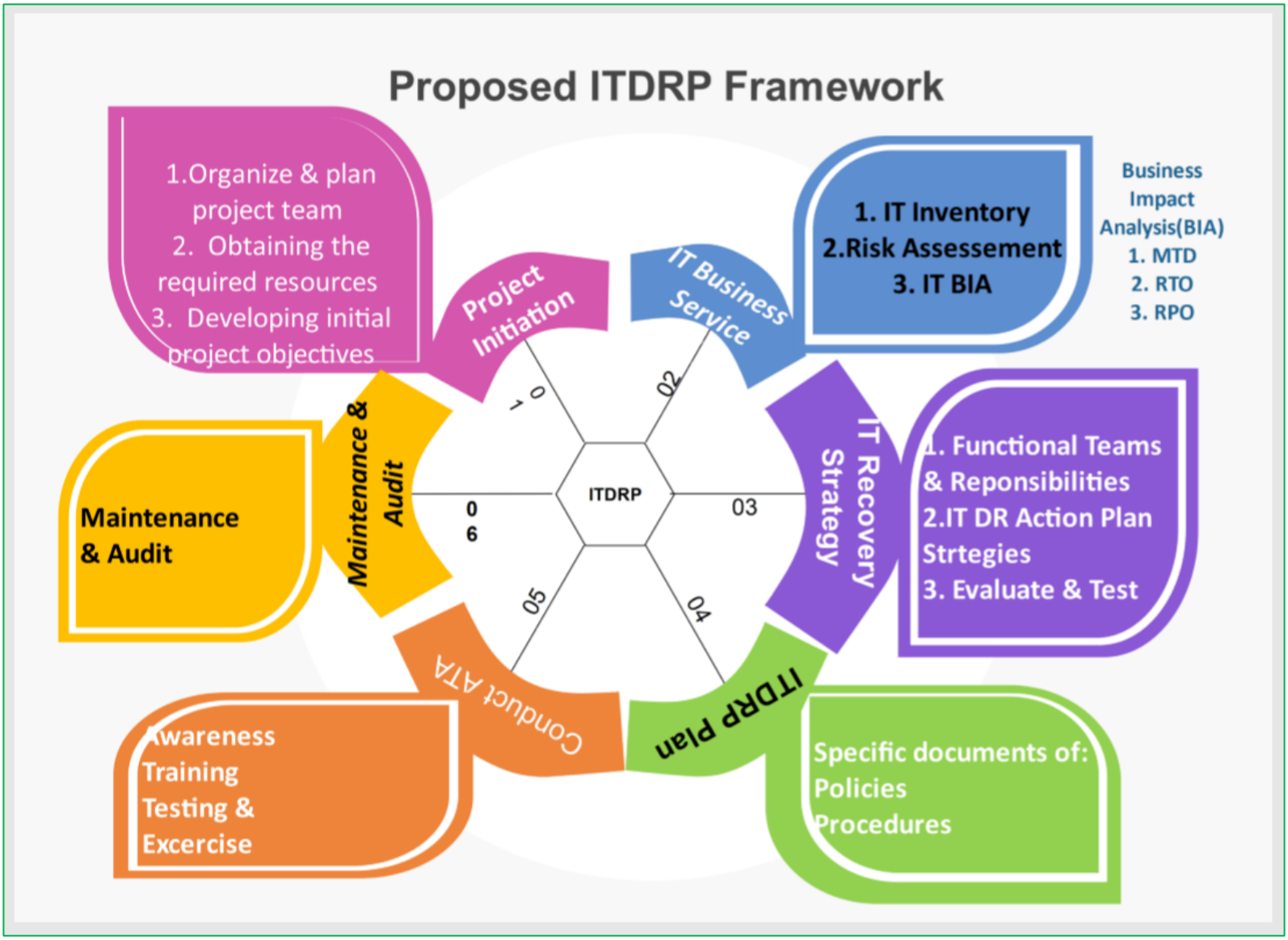


Fig. 4.1. Final Proposed IT DRP Framework

4.7. CHAPTER SUMMARY

In this chapter, the data gathered from the participant of the study was analyzed, presented and discussed. The gaps and challenges for information technology disaster recovery in the banks has been identified. The ITDRP framework is validated by the Bank's area experts. In general, preparing a corporate contingency plan is a non-stopping endeavor. However, bank leaders, board members, and CIOs must recognize the vulnerabilities they invite by not adequately planning for survival. IT disaster planning is surely a crucial part of the overall business plan. If a bank business is to survive, strategic and tactical planning in line with IT recovery planning is essential. The final corporate IT DRP plan is the lifeblood of a bank's survival. However, it is only as good as the foundation upon which it was built. The foundation is, of course, the concept and the concept is IT DR plan.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

5.1. INTRODUCTION

This chapter revises and discusses the summary of key findings, the limitation of the study, conclusions and recommendations. Further studies have been forwarded for future study to help other researchers deeply explore or extend the existing study to other sectors.

5.2. SUMMARY OF KEY FINDINGS

The IT DRP in the banking industry is important for recovering the lost data and customer information during disastrous scenarios as well as events of artificial, natural disasters, and technological failures. Literature indicated that the main purpose of a bank is to maximize revenue and to create value for stakeholders and customers by providing a wide range of banking services and secure platforms for these services through the effective management of risk (Al-Tamimi and Al-Mazrooei, 2007). If Ethiopian Banks fail to consider a range of scenarios and fail to develop a range of recovery options that would enable the bank to recover from these shocks, the adverse result would be shocking by itself. As identified by the literature, disasters that shut down a bank's mission critical applications for any length of time could have devastating direct and indirect negative effects to the bank, the country and its economy that make considering an IT disaster recovery plan essential (Montri and Kitti, 2008). It was also mandated by the Bank's supervision like Basel Committee on Banking Supervision that all banks should have contingency and recovery plans in place to ensure that they could continue to operate after disaster and limit losses in the event of a catastrophic business disruption scenario.

The purpose of this research was to identify the gap in the Ethiopian banks IT disaster recovery, understand the existing IT disaster recovery practices and challenges, and compare them with international standards, regulatory guidelines, and other important aspects in order to come up with a proposed framework solution at the end of the day. The study was conducted as a qualitative approach and data were collected by structured interview. Case study was used to select and represent the government and private owned banks in Ethiopia. A detailed literature review was

conducted in order to identify IT DRP concepts. ITDRP concepts have been identified and described to conceptualize the Ethiopian Bank's proposed conceptual framework. An interview protocol has been devised and set from the proposed conceptual framework and face to face and phone interview has been made with IT audit directors, CIOs, BC and DR managers, IT security directors, IT security managers, Risk managers, etc. of selected government and private owned Banks in Ethiopia.

The interviewees in case of both banks said that there is no IT DRP developed and in its full form. Both banks have initiated the IT DRP project and still there are gaps and limitations that drawback the bank from developing the plan.

The majority of the participants in both cases stated the cause of the draw-back was lack of focused group. There were no business continuity and IT disaster recovery planning department established in the bank who give due consideration for the development of the plan which is currently an issue for Bank B. Even though Bank A has established the BC and IT DRP department, there is still a knowledge gap, lack of experiences, trained human power, management lack of enforcement, and technology gap exist as an issue. It was also found from the interview that adopting an international standard is an issue. Participants of both Banks agreed on the difficulties of the direct implementation of the international standards due to its coverage area limitation, lack of details and implementation experience to fit the culture and context of each bank.

The type of IT disaster recovery can be driven by business impact analysis which contains three major metrics such as MTD, RPO and RTO. It was found that both banks did not conduct BIA and did not determine the metrics. The main reason behind this fact was the backbone of the telecom infrastructure of the country could not carry the full data replication and synchronization between data center and recovery site.

In general the following IT DRP challenges have been identified from both banks in the course of conducting the interview with the participants.

- ✓ Lack of focused group both from IT side and management side
- ✓ Lack of experiences and IT DRP educated personnel in the bank and on the market
- ✓ Lack of training and awareness
- ✓ No certified IT DRP implementation company in the country

- ✓ Lack of IT DRP standardization in the country
- ✓ Lack of guaranteed telecom infrastructure backbone
- ✓ No established business continuity and IT disaster recovery department
- ✓ Lack of IT DRP educational academy or university
- ✓ Lack of advisee's linkage between banks and educational entities
- ✓ Lack of IT DRP framework in the banking sector in Ethiopia
- ✓ priority is not given to IT DRP by bank's management and board of members giving much attention to core business of the bank
- ✓ unavailability and expensive ness of critical hardware and software systems
- ✓ limitation of separate IT risk analysis team

5.3. CONCLUSION

The objective of the study was to propose a framework for Ethiopian Banks ITDRP that can be used as a base for developing their respective disaster recovery plan by identifying current practices and challenges and assessing other frameworks done elsewhere. According to the plan, the assessment of current practice was made and challenges were identified from one government owned and other private owned banks in Ethiopia. Per the study the strength of Bank A related to the study is the establishment of IT business continuity and disaster recovery department which deals with any IT disruption scenarios. Other strength of Bank A is that it has a well-established IT security directorate and IT audit directorate with sub sections to deal with IT security issues and IT audit and evaluation activities respectively. An added strength of Bank A is the implementation of an automated asset management software to deal with IT inventory systems which is one component of IT DRP plan documents. The follow up of the IT audit to necessitate the development of IT DRP is the strength of both Banks and regulatory bodies like the national bank of Ethiopia. According to the participant's reply to the interview questions, the limitation of guaranteed strong backbone network between data center and recovery site provided by service providers in the country is a challenge to both banks.

Both banks have initiated the project to develop IT DRP which the study appreciates as a starting point. But the knowledge gap, lack of experience, technology gap and other challenges listed in

the previous chapter has limited the banks from fully developing and implementing the IT DRP plan. In general, the efforts to develop the IT DRP for banks of Ethiopia provides an initial first step towards a better understanding of the complexities of IT disaster recovery planning in the banks as well as other financial sectors in Ethiopia.

Therefore, in attempt to answer the research questions, the study has been able to: 1) identify current practices and challenges of the banks 2) assess other frameworks from literatures 3) identify elements of IT DRP per international standards and models 4) develop the proposed descriptive and prescriptive framework for Ethiopian Banks 5) evaluate the proposed framework by area or domain experts. Based on the analysis and findings, the following points are concluded.

- ✓ If IT DRP is not in place, ability to recover systems and restore lost critical-data is impossible and there is subsequent financial and economic loss to the banks and the country
- ✓ Clearly identifying and prioritizing critical, dependency requirements and essential business functions and IT systems are the ability to deliver sound banking services that depend on systems and gaining community and customer confidence that proudly rely on the bank's best service.
- ✓ Recovery time objective and recovery point objective determines bank's ability to provide the basis for identifying and analyzing viable strategies for inclusion in the IT DRP plan
- ✓ Recovery strategies allow banks to quickly respond to crisis and recover as many critical-functions and systems as possible.
- ✓ Pre and post training, awareness and exercise ensures the capability and skills of the IT DRP team to relocate and restore before and after disruptions and disastrous scenarios.
- ✓ Audit and maintenance of IT DRP document eliminates obsolescence technology and services and cope up with new systems which is directly proportional to fast relocation and restoration of critical services and data.

5.4. LIMITATIONS

The study is limited by the current level of understanding of the IT DRP plan document development, implementation, training, testing and updating in the country in general and in the Banks in particular. Some of the topics except pre-planning phase such as project initiation and risk analysis are difficult to gather sufficient data about in order to present a representative answer. Planning phase and post planning phase are not developed and implemented in both cases. This resulted in limited explanation on the rest of subject areas.

The interview attempted to be conducted with the Bank's risk management directorate, one bank's CIO and IT security directorate was not achieved due to the inconvenient time and out of office for training and other reasons. One private bank was totally dropped because of study denial by the bank. Besides, the study is limited to one tool that is interview as the document analysis and observation was not available and possible so that triangulation was not achieved per the plan.

Banks were not willing in some cases to admit weaknesses in security measures and do not want to share information that can be used to expose vulnerabilities concerning IT risk analysis and assessment. In most cases, the banks were willing to share information regarding the topic.

5.5. RECOMMENDATIONS

The importance of IT DRP for the Bank is unquestionable. Ethiopian Banks should re-consider the development and implementation of IT DRP processes, policies and procedures to reduce the impact of IT disasters and system failures to an acceptable level and be able to mitigate the disruptive scenario through preventative and recovery measures. The preventive and recovery measures should identify, reduce, and protect the system from probability of the risk to occur and should limit consequences of damaging incidents like cyber-attack. Based on the current practices and challenges identified in both cases and the proposed ITDRP framework steps or process, the following are recommended so as to help the banks to develop and implement the IT DRP plan documents.

1. Banks must establish the need for IT disaster planning in line with business strategies and initiate a project plan to guide the development process to assure the success of the resulting DR plan.

2. Banks should determine the IT business impact analysis and set the maximum tolerable downtime, the recovery time objective and recovery point objective of each critical, essential and non-essential processes they have identified.
3. The banks should define and specify the approach, policies, procedures, and standardization of strategies that span the hardware, software, facilities and human elements involve in the pre-disaster, during disaster and post disaster activities to swiftly and efficiently recover from any crisis type that halt the business functions of the bank.
4. The Banks require to identify and document specific procedures of selected risk management and response team members with roles and responsibilities, defined disaster severity levels and recovery process and identified activation triggers specified in the strategies development to be invoked in the event of a disaster to develop an effective DR plan.
5. The Ethiopian Banks can take the currently developed IT DRP framework as a major input to help them develop their own respective IT DRP plan
6. The bank should conduct quarterly or bi-annual as needed, IT DRP testing, training and awareness to ensure the plan is working as planned.
7. The constant maintenance and update of the IT DRP plan should be conducted to keep the consistency and validation of the document with current technology and systems.
8. IT technology and IT DRP audit should be done to evaluate the currency of technology, documents and systems.

5.6. FUTURE WORKS

In order to cope up with the current advance in cyber-attacks, threats and risks of IT related disasters the following further issues are recommended for future research to benefit the banks and other financial organizations in the country.

1. IT DRP framework for financial sectors and industries. The study can be extended with limited assessment as this research is limited to technology and culture of Banks and not included sectors like microfinance, insurance, etc.
2. Multi-vendor outsourcing, multi-vendor cloud, and multi IT solutions DRP framework for banks and financial sectors. This study is undertaken with regard to current technologies exist in the banking sector. Further study will be needed if the technology transfer happens in the banking sector of Ethiopia.
3. Business continuity and disaster recovery framework for banks and financial sectors. The scope of this study is limited to IT DRP and does not include the business continuity plan.
4. The role of educational institution in solving scarcity of BC and DR professionals in the financial and other sectors. One of the main challenges in the banking sector identified in the study is the scarcity of IT DRP professionals on the market.
5. IT DRP framework implementation for financial sectors in Ethiopia.

References

1. Abramson, D. M., Grattan, L. M., Mayer, B., Colten, C. E., Arosemena, F. A., Bedimo-Rung, A., & Lichtveld, M. (2015). The Resilience Activation Framework. The Journal of Behavioral Health Services & Research, 42(1), 42–57.
2. Acronis International. (2016). System and method for rapid restoration.
3. Adedayo, O. (2014). Disaster Recovery Strategy and Maintenance Plan.
4. Aggelinos,G. and Katsikas, K. (2011). Enhancing SSADM with disaster recovery plan activities.
5. Ali, Y. (2011). Quality in Qualitative Studies: The Case of Validity, Reliability and generalizability.
6. Alhazmi, O. and Malaiya, Y. (2013). Evaluating disaster recovery plans using the cloud.
7. Al-Tamimi, H. and Al-Mazrooei, M. (2007). Banks' Risk management, The Journal of Risk Finance Incorporating Balance Sheet, 8(4), 394-409.
8. Ashebir E. (2017). Assessment of Information Systems continuity Management at commercial Bank of Ethiopia.
9. Bajgoric, N. (2006). Information technologies for business continuity. An implementation Framework.
10. Balaouras, S. (2009). The State of Business Continuity Preparedness.
11. Bank of Tanzanya, (2009). Business continuity management guidelines for banks and financial Institutions.
12. Basel Committee on banking supervision. (2009). Enhancement to the Basel II framework.
13. Baškarada, S. (2014). Qualitative case study guidelines. The qualitative report, 19(40).
14. Benjamin, O. (2014). ITDR and Business Continuity at UN in Kenya.
15. Bradbury, C. (2008). Disaster! Creating and testing an effective recovery plan.
16. BSI Standard BS ISO 22301. (2012). Societal security – Business continuity management systems – Requirements.
17. Bryman, A. and Bell, E. (2006). The Ethics of Management Research: An Exploratory Content Analysis.

18. Carer-steel, A. and Pollard, C. (2009). Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study.
19. Choudhary, R. and Bhattacharya, D. (2016). Business Continuity Planning: A Study of Frameworks, Standards and Guidelines for Banks IT Services. International Journal of Emerging Research in Management &Technology, 5(8), 33-40.
20. Clarke, V. and Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning.
21. Collins, J. and Hussey, R. (2014). Business Research: Understanding Research.
22. Creswell, W. (2003). Research design: Qualitative, quantitative, and mixed methods design. Sage, London.
23. Cropley, A. J. (2019). Qualitative research methods.
24. Denzin, K., and Lincoln, S. (2011). The Sage handbook of qualitative research. Thousand Oaks, CA: Sage.
25. Edmonds, A., and Kennedy, D. (2012). An applied reference guide to research designs Quantitative, qualitative, and mixed methods. Thousand Oaks, CA: Sage.
26. Ethiopian ICT Development Agency. (2008). National disaster prevention and recovery plan and procedure.
27. Gerring, J. (2008). Case selection for case-study analysis: Qualitative and quantitative techniques.
28. Ghannam, M. (2018). Challenges and Opportunities of Having an IT Disaster Recovery Plan.
29. Glen, B. (2009). Document Analysis as a Qualitative Research Method.
30. Goiri, I., Le, K., Haque, E., Beauchea, R., Nguyen, T., Gutart, J. and Torres, J. (2011). Scheduling energy consumption in green datacenters.
31. Gray, C. and Malins, J. (2004). Visualizing research: a guide to the research process in art and design.
32. Gregory, Peter (2013). IT Disaster Recovery Planning For Dummies. (PP. 10-14).
33. Grembergen, V., Haes, D., and Moons, J. (2005). Linking Business Goals to IT Goals and COBIT Processes. Information Systems Control Journal.
34. Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. The Qualitative Report, 8(4).

35. Guidelines for Information and Communications Technology Disaster Decovery Services. (2008E). ISO/IEC 24762:2008(E).
36. Guidry, P., Vaughn, D., Anderson, R., and Flores, J. (2015). Business Continuity and Disaster Management. Mitigating the Socioeconomic Impacts of Facility Downtime after a Disaster. IEEE Industry Applications Magazine, 21(5), 68–77.
37. Haylay G. (2018). An investigation of current status of IT Disaster recovery Plan in Ethiopian Banking Sector.
38. Hawkins, S., Yen, D. and Chou, D. (2009). Disaster recovery planning: a strategy for data security. *Information Management & Computer Security*, 8(5), 222-230.
39. Hill, E., Knox, S., Thompson, J., Williams, N., Hess, A., & Ladany, N. (2005). Consensual qualitative research: An update. *Journal of Counseling Psychology, 52*(2), 196–205.
40. Hoffer, J. (2001). Backing up Business-industry Trend or Event. Health Management Technology, 22(1).
41. ISACA, COBIT 5. (2012). Enabling Processes (1 ed.).
42. ISO/IEC 27031. (2011). Information security – Security techniques – Guidelines for information and communication technology [ICT] readiness for business continuity.
43. ISO/IEC 24762. (2008). Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services.
44. Jabareen, Y. (2009). Building a Conceptual Framework: Philosophy, definitions, and Procedure. International Journal of Qualitative Methods, 8(4).
45. John, W. and James, R. (2005). Business continuity and disaster recovery for info-sec Managers.
46. Jones, V. A. (2011). How to Avoid Disaster: RIM's Crucial Role in Business Continuity Planning. *Information Management Journal*, *45*(6), 36-40.

47. Joseph, J. (2016). IT-DRP for Business Continuity: Case Study in a Business Sector.
48. Kadlec, C. and Shropshire, J. (2010). Best Practices in IT Disaster Recovery Planning Among US Banks. Journal of Internet Banking and Commerce, 15(1), 1-11.
49. Kajornboon, A. (2005). Using interviews as research instruments.
50. Kappelman, L., McLean, E., Johnson, V. and Gerhart, N. (2014). The 2014 SIM IT Key Issues and Trends Study. *MIS Quarterly Executive*: 13(4).
51. Karim, A. (2014), Data Collection Instruments.
52. Kimberlin, L. and Winterstein, G. (2008). Validity and reliability of measurement instruments used in research. Am J Health-Syst Pharm, 65, 2276-2288.
53. Koskei, B and Simiyu, C. (2014). Role of Interviews, Observation, Pitfalls and Ethical Issues in Qualitative Research Methods.
54. Kothari, C.R. (2004). Research Methodology: Methods & Techniques. Second edition. New-Delhi: New Age International.
55. Kozina, M. (2009). COBIT - ITIL mapping for Business Process Continuity Management, in Central European Conference, Vara˘zdin.
56. Kimberlin, C. and Winterstein, A. (2008). Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy*, 65 (23).
57. Kuamoo, P. (2006). A framework for evaluating IT service management software products.
58. Lanter, A. (2011). Are You Ready? Getting Back to Business after a Disaster. I*nformation Management Journal*, *45*(6).
59. Leong,H. and Govindan, M. (2014). Critical Dimensions of Disaster Recovery Planning, International Journal of Business and Management, 9(12).
60. Luckey, T. (2009). Key Stages of Disaster Recovery Planning for Time-critical Business Information Technology Systems.

61. Loftness, S. and Drapeau, M. (2007). Contingency Planning & Management.
62. Mackey, A & Gass, S.M. (2005). Second language Research: Method and Design. London Lawrence Erlbaun, Associate Publishers, Mahwah.
63. Maitra, S. Shanker, M. and Mudholkar, K. (2013). Business Continuity and Disaster Recovery Experience in Indian Banks. International Journal of Latest Trends in Engineering and Technology (IJLTET), 2(4), 526-534.
64. Marks, D. and Yardly, L. (2004). Research methods for clinical and health psychology.
65. Martin, B. (2002). Disaster Recovery Plan Strategies and Processes.
66. Menkus, B. (1994). The New Importance of 'Business Continuity' in Data Processing Disaster Recovery Planning. Computers & Security, 13(2), 115-118.
67. Mohammed, E. (2009). Evaluating Business continuity and Disaster recovery planning in information technology departments in Palestinian listed companies.
68. Mohamed, R. (2014). A Proposed Model for IT Disaster Recovery Plan. I.J. Modern Education and Computer Science, 4, 57-67.
69. Montri, W. and Kitti, K. (2008). Optimization strategy for disaster recovery.
70. Myers, M. (2019). Qualitative research in business and management.
71. NBE (2012). History of Ethiopian Banking. Insurance, Banking and Negotiable Instrument Law, Addis Ababa.
72. Nigussie B. (2017). Assessment of IT Disaster Recovery Practices in Ethiopian Commercial Banks.
73. Nijaz, B. and Moon, Y. (2009). Enhancing systems integration by incorporating business continuity drivers.
74. Otero, A. (2018). Information Technology Control and Audit.
75. Partio, A. (2014). Data center Disaster Recovery & Major Incident Management.
76. Prazeres, S. and Lopes, E. (2013). Disaster Recovery: A project planning case study in Portugal, Procedia Technology, 9, 795–805.
77. Protiviti. (2017). Guide to Business Continuity management (3rd ed.).

78. Randeree, K., Mahal, A. and Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Mgmt Journal*, 18(3), 472-492.
79. Rocco, T. and Plakhotnik, M. (2009). Literature Reviews, Conceptual Frameworks, and Theoretical Frameworks: Terms, Functions, and Distinctions. Human Resource Development Review, 8(1),120-130.
80. Rothstein, P. (2007). Disaster recovery testing: Exercising your contingency plan.
81. Sapsford, R. and Jupp, V. (2006). Data collection and Analysis.
82. Saunders, M. and Lewis, P. (2012). *Doing Research in Business & Management: An Essential Guide to Planning Your Project.*
83. Sheth, S., McHugh J. & Jones, F. (2008). A Dashboard for Measuring Capability when Designing, Implementing and Validating Business Continuity and Disaster Recovery Projects. Journal of Business Continuity & Emergency Planning, 2(3), 221-239.
84. Somasekaram, P. (2017). A Component-based Business Continuity and Disaster Recovery Framework.
85. Sonal, C. (2005). Internet Banking In India: A glimpse of its adoption and implementation in India through case studies.
86. Spencer, R. and Johnston, R. (2003). Technology best practices.
87. Snedaker, S. (2013). Business continuity and disaster recovery planning for IT professionals.
88. Sudhish, R. (2013). Optimization of Disaster Recovery Leveraging Enterprise Architecture Ontology.
89. Susan, S. (2007). Business continuity and disaster recovery planning for IT Professionals.
90. Swanson, M. et al. (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Revision 1.
91. Telovations. (2012). Breakdown. Disaster recovery and business continuity. Retrieved from https://telovations.wordpress.com/tag/revenue-lost-due-to-natural-disaster/

92. Teuten, C. (2005). The top ten mistakes in risk management. Financial Executive, 45-45.
93. Tipton, H. and Krause, M. (2007). The maturity evaluation framework developed for contingency planning.
94. Uddin, M., Hapugoda, S. and Chand Hindu, R (2015). Disaster Recovery Framework for Commercial Banks in Sri Lanka. J. ICT Res, 9(3), 263-287.
95. Verhofstad, J. (2000). Recovery Techniques for Database Systems.
96. Yin, R. (2009). Case study research: Design and methods (4th Ed.). Thousand Oaks, CA: Sage.
97. Ylikangas, M. (2017). Assessing maturity of disaster recovery planning. A case study.
98. Zainal, Z. (2007). Case study as a research method.
99. Ziyad, Mohamed G. (2017). Challenges and Opportunities of Having an IT Disaster Recovery Plan.
100. Williams, C. (2007). Research Methods. Journal of Business & Economic Research, 5(3), 65- 72.
101. World Disaster Report. (2010). The Global Risk Report.
102. World Economic Forum. (2019). The Global Risk Report.

APPENDICES

Appendix A: Interview Questions

Table Interview Questions by each area.

Area	Questions
Project Initiation	In what circumstances was the IT disaster recovery planning initiated in your bank? What was the role of the management in starting ITDRP project? How did you organize the project team? What was the challenges of initiating the project
IT Inventory	How do you conduct IT inventory in your Bank? Have you identified all IT services in all departments? Have you ranked the order of IT services to recover if IT disasters occur?
IT Risk Assessment	What kind of formal analysis was identified and conducted on the criticality of the services included in the disaster recovery planning? Is the continuity of assessing potential risks of disaster that impacts the IT applications and systems an always task in your bank? What is the challenge of assessing risks in your bank?
IT Business Impact Analysis	Were the impacts of disruption and estimated downtime assessed in your formal analysis? Were the resources included in the service mapped? Were the priorities in the service discussed? What kind of service level agreements do you have in place and with whom? Your RPO and RTO?
Recovery Strategies	What preventive controls are in place? Are they technical or administrative in nature? What kind of backup and restoration strategies are there? What is the expectation of data loss in case of disruption? Are there alternate sites? What is their role in contingency?

	Do you have a procedures of a relocation? Do you have procedures of physical facilities such as IT building, power and cooling systems? Do you have an established functional team and their responsibilities? Do you have an explicit chain of command for dealing with IT disasters? How do you assess IT damages, support customers, and communicate during emergencies? How do you do a site test? What kind of facility and human aspect are available on site? What are the challenges of recovery strategies?
Disaster Recovery Plan	What kind of disaster recovery plan has been written? What do they contain? Have you referred to any standards, models or guidelines? Is it in line with a strategic business perspective? Do you have documented specific policies and procedures in place? What are the challenges of developing disaster recovery plan documents?
Test, Awareness, Train and exercise	What kind of approach was taken in testing the disaster recovery plan? How was the training conducted? What awareness techniques are used? What kind of exercises have been there? How often tests and exercises are conducted? Any challenges related to awareness and training?
Maintenance and Audit	Are the DRP changes updated? What is the input for plan maintenance? Are you auditing your IT DRP plan? How?

Appendix B: IT disaster emergencies and its effects declared around the world

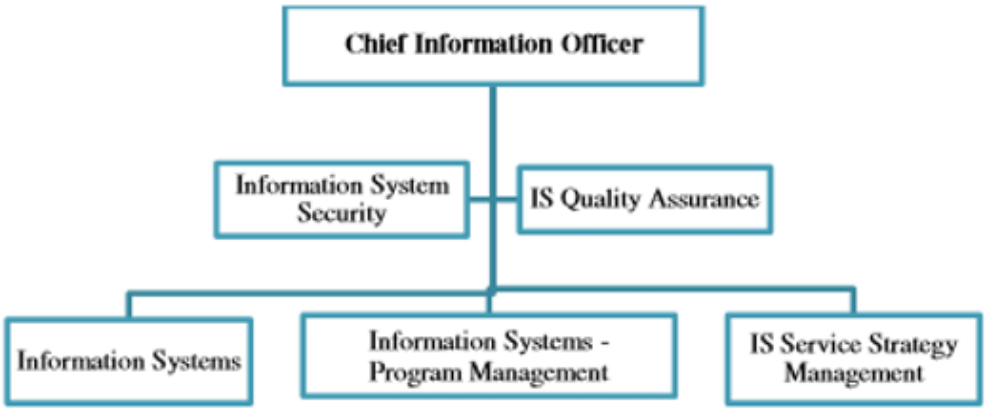
No	year	Emergency	Country	Effect
1	2000	Crash of computer systems globally with the beginning of the year 2000, widely known as the Millennium Bug	Global	An estimated amount of £400 billion were spent on the recovery operations (as projected by the house of commons)
2	2005	Failure of the cargo system in 2005 at the customs service in Australia	Australia	Due to the failure, cargo was left unattended over many days leading to global delays. An overall cost of USD 200 – 250 million was utilized for recovery.
3	2007	Faulty network card at USCBP (US Customs & Border Protection) led to sharing of incorrect data across the airlines network	USA	Standstill at the Los Angeles airport leading to a grounding of all flights.
4	2007	Failure of the health payroll system by the technical failure of the system developed by tech giant IBM, against a contract worth USD 6 million	Australia	The failure resulted in mismanagement of salaries of health care professionals accounting to 80,000 in Queensland healthcare system.
5	2013	IT emergency due to failure of the system to accommodate the huge influx of visitors to access health care facilities	USA	Health care services were disrupted leading to heavy dependency of the users on outdated technology
6	2013	IT emergency due to crash of the widely used worldwide travel reservation system	Global	The global aviation industry was in a shock due to the crash leading to delays and cancellations by over 300 airlines
7	2014 - 2015	Anthem Inc. became the victim of the biggest hacks in the financial services industry.	USA	37.5 million Records of almost 80 million people stolen which costs $115 million.
8	2015	UK telecommunications and internet service provider TalkTalk attack	UK	157,000 personal details were stolen and cost €77 million. Loss of 90,000 customers.

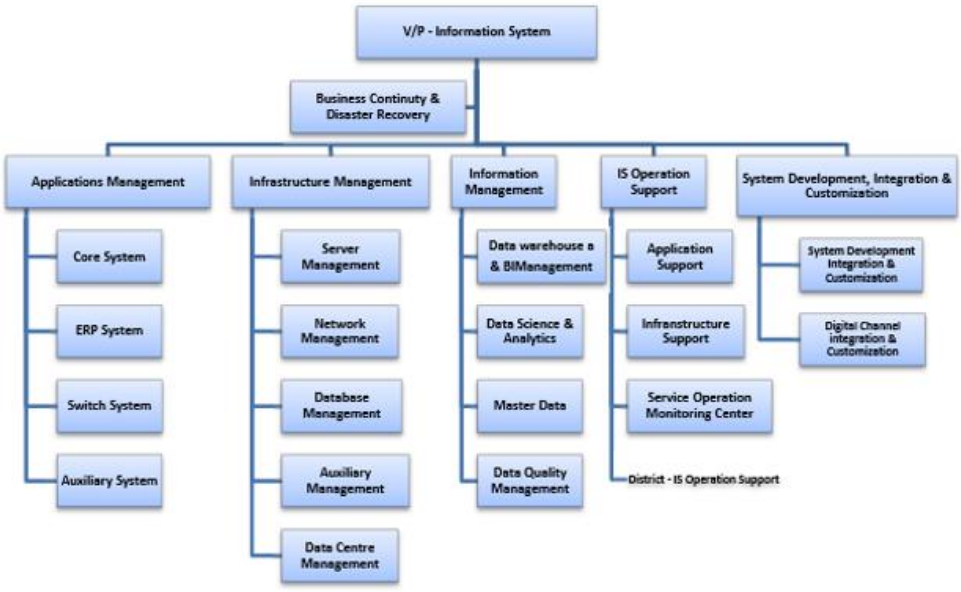
9	2017	Ransomware cyber-attack affecting operations of government, private firms, banking institutions globally	Global	The overall network and operations were paralyzed with the cyber-attack, demanding a ransom and threatening to leak sensitive private information to the public.
10	2018	Data breach at Starwood division of Marriot	Australia	Losses of US dollars between $200 and $600 million.
11	2018	City of Atlanta was struck by ransomware known as SamSam	USA	Costs $2.7 billion and essential city systems were taken offline, some (such as managing traffic-ticket system hearings) did not come back online until mid-April
12	2018	Exploits aimed at gaps or weaknesses in Facebook's code.	Global (Facebook)	50 million Facebook users were potentially affected and the cost was undisclosed.
13	2019	A disaster by crash of Boeing 737-max causes Tsunami of alerts on flight display-IAS-DISAGREE the flight computer has detected a sensor malfunction defective error. MCAS software was the focus of the investigation.	USA, Ethiopia and Indonesia	346 people killed. Boeing's shares failed 6% and paid $5 billion cost of compensation. Many planes have been banned.

Source: (Barker (2017); Financial Review (2017); ACCA (2019); Financial Review (2019); CNN)

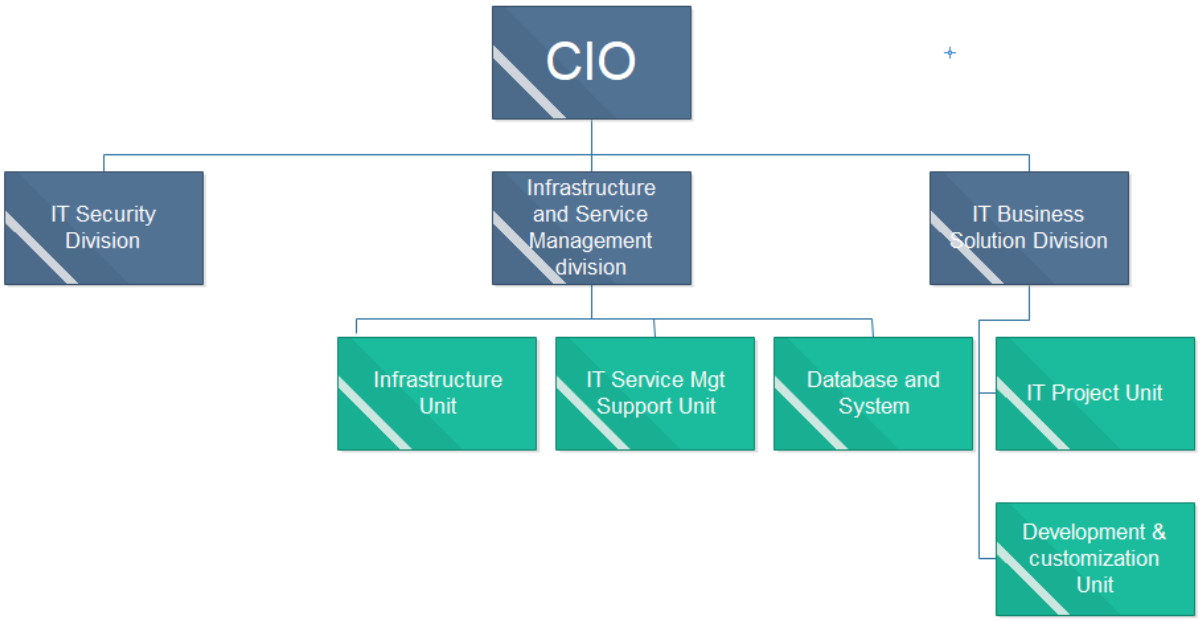
Appendix C: *IT Structure of Bank A and B*

Bank A:

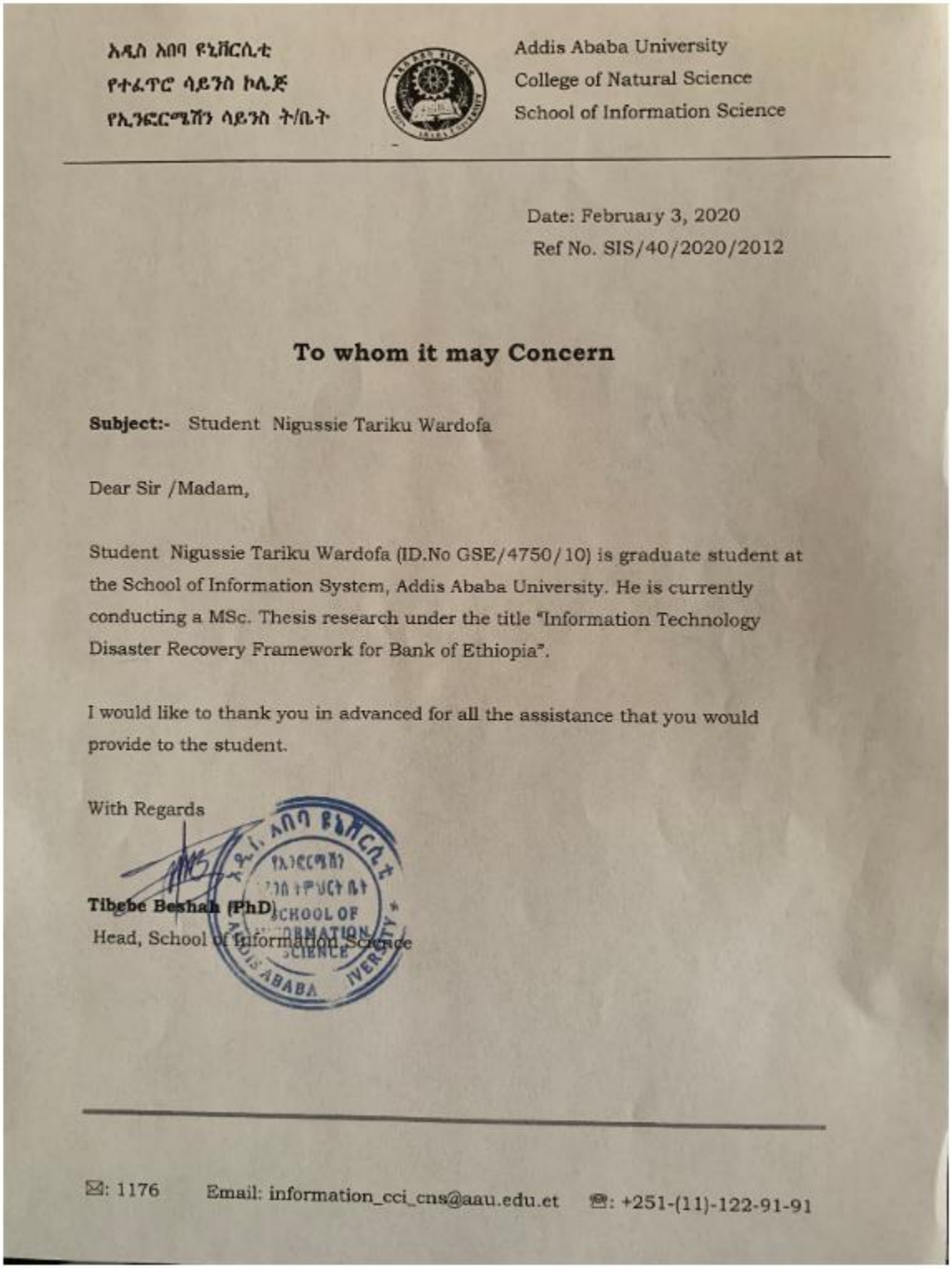




Bank B:


CIO
IT Security Division
Infrastructure and Service Management division
IT Business Solution Division
Infrastructure Unit
IT Service Mgt Support Unit
Database and System
IT Project Unit
Development & customization Unit

Appendix D: Support Letters to Ethiopian Banks



አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

Addis Ababa University
College of Natural Science
School of Information Science

Date: February 3, 2020
Ref No. SIS/40/2020/2012

To whom it may Concern

Subject:- Student Nigussie Tariku Wardofa

Dear Sir /Madam,

Student Nigussie Tariku Wardofa (ID.No GSE/4750/10) is graduate student at the School of Information System, Addis Ababa University. He is currently conducting a MSc. Thesis research under the title "Information Technology Disaster Recovery Framework for Bank of Ethiopia".

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

✉: 1176 Email: information_cci_cns@aau.edu.et ☎: +251-(11)-122-91-91

የኢትዮጵያ ንግድ ባንክ

COMMERCIAL BANK OF ETHIOPIA

INTER DEPARTMENTAL MEMORANDUM

DATE ቀን	:	**February 14, 2020**
TO ለ	:	**Director – IT Security**
FROM ከ	:	**Team Leader – Training Operation**
SUBJECT ጉዳይ	:	**Request for Cooperation**

Addis Ababa University has requested our bank to assist and cooperate student **Nigussie Tariku Wardofa** to grant access to the required information to the research work entitled **"Information Technology Disaster Recovery Framework for Commercial Bank of Ethiopia."**

This is, therefore to request you to provide him the required assistance and cooperation without compromising confidentiality.

With Regards

Achamyelesh Borshe

/ma

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date:- February 14, 2020
Ref: - SIS/40/2020/12

To:- Commercial Bank of Ethiopian

Dear Sir/Madam,

Student Nigussie Tariku (ID.No GSE/4750/10) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "Information Technology Disaster Recovery Framwork for Bank of Ethiopia".

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

✉: 1176

☎: +251-(11)-122-91-91

Appendix E: Descriptions of stages and areas of MAM

Stages	Name	Description	Areas	Description
Stage 1	Uncertainty	Threats are not analyzed or understood, prevention, detection and recovery are not formally addressed. Contingency planning usually consists only of personnel evacuation plans and simple procedures such as backup and restore procedures.	Management	Management does not use risk assessment for incident reduction and does not understand the necessity of contingency planning by blaming circumstances which caused the incident
			Organization	There is no organization or function for contingency planning.
			Incident	Incident handling is reactive rather than proactive. Even a minor incident could be disastrous
			Economics	Minimal or no funds spent on prevention, the loss is unmanaged and unpredictable.
			Improvement	No organized contingency planning improvement nor risk reduction activities
Stage 2	Awakening	The realization of IT disaster recovery planning has some value, and the realization of inability brings out the need to provide resources to support planning. The initial focus may be on the most dramatic threat while ignoring the more probable and significant threats.	Management	Relying on technical solutions
			Organization	Contingency planning function may be appointed with the main emphasis being coordination of file backup and restores
			Incident	Handles incidents and the basic statistics are gathered on major incidents.

			Economics	Preventive actions are minimal; the impact of the incidents is unpredictable.
			Improvement	Enterprise policies start to emerge for handling most obvious threats.
Stage 3	Enlightenment	Disaster recovery planning is understood to be necessary, and the resource allocation for the planning is more realistic. The first business impact analyses are attempted and relevant disaster scenarios are developed	Management	Management understands that the DRP is necessary for maintaining the service levels. Management supports focus on most critical assets and infrastructure
			Organization	The contingency planner develops corporate policy and implements training
			Incident	Better statistics providing clearer view to the threats
			Economics	Preventive actions aim to assure the IT service levels
			Improvement	End users have confidence for ability to restore systems. End users expect and rely on higher service levels
Stage 4	Wisdom	The business has focus in this stage. Now management visibly participates in the planning. Business units are encouraged to participate. Organizationally contingency planning moves under information security function. Threats are re-evaluated continually based on evolving threats. Legal perspective is considered for each type of incident.	Management	Management makes informed decisions. Management encourages business units to identify the requirements for their critical business functions.
			Organization	The contingency planning transitions into information security function
			Incident	Threats are continually assessed based on threat population and

				security incidents. Legal actions are planned for each type of incident
			Economics	Preventive actions are continuously managed. Periodic risk analysis undertaken. Reduced losses.
			Improvement	Risks are evaluated accurately. Accurate business impact analysis.
Stage 5	Certainty	Continuous improvement regarding the processes and participation in public and professional forums. Management fully supports the contingency planning program. Research and development are funded. Top management participates and is aware of contingency planning programs. Prevention strategies are fully developed. Proactive contingency planning is in place and continuously refined	Management	Management understands and Adequate resources are provided
			Organization	Information security officer regularly meets with higher management. Process improvement is a concern
			Incident	The causes of business interruptions are determined. Incident data is taken into account in the risk management
			Economics	Prevention is justified. The stability becomes recognized. The loss is minimized.
			Improvement	Business continuity actions are considered as normal. Process improvement often comes from the end users.

Appendix F: Comparison of different International standards.

Standards	Common use	Differences and Similarities	Strengths	Weaknesses
COBIT	Employed by business executives to successfully execute key policies and procedures. Additionally, it is often used to tie together controls, technical issues and risks within an organization.	COBIT is a high-level framework (relative to ITIL, ISO and NIST) that maps core IT processes in a manner that allows governance bodies, usually business executives, to successfully execute key policies and procedures. Similar to ISO, it answers the 'what' that is being managed, as opposed to the 'how' answered by ITIL. However, ITIL and ISO are focused only on information security, COBIT allows for a much broader scope, taking into account all of IT management and IT contingency processes.	COBIT is managed by ISACA and keeps the standard up-to-date and on-par with current technology. It is a globally accepted standard and encompassed far more than just the information security scope that other standards are limited to. It is also easier to partially implement COBIT without requiring a full-spectrum analysis and commitment by the organization.	While being widely scoped it can be viewed as a strength for COBIT, it can also be a detractor during implementation. Being by design not limited to a single area, it can often lead to gaps in coverage.
ITIL	Originally designed for use within the U.K. government and is most applicable within that realm. However, it is now a globally accepted standard and is in-use by many companies outside the geographical area of origin.	ITIL is a set of best practices an organization may implement in order to align IT resources and offerings to business goals. It is offered in a series of five core publications each corresponding to a stage in the lifecycle of IT. This process produces documentation of processes, tasks and checklists not specific to the organization with a goal of being able to create a baseline from which to implement controls and measure success.	ITIL is created and managed by the U.K. government, and is a natural fit for companies in that area of the world. However, the ITIL standard is used worldwide and may be considered for any company regardless of geographical location. ITIL excels at increasing visibility into and management of internal process to positively impact efficiency and economy.	While focused on information security only, ITIL is considered to be a higher-level standard than ISO, and points to ISO standards for detailed implementation. Specific implementation details are rather lacking.
ISO	Commonly used by or in accord with an	ISO provides best practice recommendations for standard	ISO recognized and understood by those	ISO is focused specifically and

	IT department specific to the organization. The IT department is the focus of the resulting management system controls.	implemented most often by using ISO.	familiar with the ISO/IEC standards. This standard allows system managers to identify and mitigate gaps and overlaps in coverage.	purposefully on information security and is therefore limited in scope compared to other standards such as COBIT.
NIST	NIST covers all steps in the Risk Management Framework that addresses the selection of security controls according to FIPS. It is used by U.S. federal organizations.	NIST Special Publication 800-53 is a requisite for federal bodies in the U.S. for security control compliance, with the exception of those associated with national security. It is published by the National Institute of Standards and Technology, and is related to FISMA (2002).	The level of detail afforded by implementing a framework based on NIST is considerable, and an organization not wishing to spend time on customizing a framework for their specific industry or nature may wish to use NIST assuming that the level of detail is complimentary to its goals.	Similar to ISO, NIST is limited in scope to information security, whereas COBIT and ITIL are more general in nature. Multiple publications must be processed and implemented in order to achieve compliance, which can lead to coverage gaps.

Appendix G: summary of related works

No	Author/s	Year	Title	Methodology	Result	Future Study	Contribution
1	Nigussie	2017	Assessment of ITDR practices in Ethiopian Commercial banks	Qualitative	Found risk gaps and ITDRP framework gaps Human aspect, plan testing, updating, international standards and preparedness are lacking in the bank.	IT DRP framework tailored to local Context of Ethiopian commercial banks and factors & challenges hold back IT DRP in the same bank.	Helps managers and banks to reconsider ITDRP and business continuity components
2	Haylay	2017	An investigation of current ITDRP in Ethiopian Banking sector	Mixed (Qualitative and Quantitative)	Identified lack of exercising ITDRP, no top management support and in-mature ITDRP.	IT DRP investigation for the financial sector, IT DRP adoption, perception of top managers and recovery and prevention strategies.	Help the banks and top managers to reassess risks and importance of ITDRP
3	Uddin et al.	2015	Disaster Recovery Framework for Commercial Banks in Sri Lanka	Qualitative	The study found banks only have ad-hoc disaster recovery standards and practices, as there is no standard framework available	To enhance the findings and include licensed specialized banks and the non-banking financial institutions to understand their disaster recovery practices as well as to develop a comprehensive framework across the country.	Helped the banks to develop standard guideline
4	Mohammed	2014	A proposed model for IT disaster recovery plan.	Qualitative	A proposed model that highlighted the basic level of IT disaster recovery planning in the field of IT	Developing the field with setting implementation that would move the planning in IT disaster recovery to its second step, as the study described its first step.	It gives IT managers highlights on how to use planning as a managerial tool in disaster recovery.

5	Shropshire &Kadlec	2009	Developing the IT Disaster recovery planning construct.	Quantitative	Identified the seven dimensions of the IT DRP Construct.	The study of post-application of DRS	The study draws attention to the adaptation of an integrated DRS. it provides a rigorously developed measure of ITDRP.
6	Hoong and Marthandan	2014	Critical Dimensions of Disaster Recovery Planning	Quantitative	The IT availability and reliability, technology competence, perceived business continuity benefits, top management support, external pressure to adopt DRP, business environment, staff competency, roles and responsibilities s were the important results	The study conducted on financial sector, and thus more study on other sectors are recommended	Stating the most important factors in DRP.
7	Prematha	2017	A Component-based Business Continuity and Disaster Recovery Framework	Design Science	Found a component based framework which eases future complex and vendor independent disaster recovery	Potential to develop and support researchers to support critical infrastructure protection	Support many IT solutions since it has software based modular approach, and it is flexible, scalable, and platform and application independent

Appendix H: Description of steps and concepts of IT DRP Framework.

ITDRP Steps	Description	Sources
1. Project Initiation	Businesses must establish the need for disaster planning and define a project plan to guide the development efforts. The major tasks included in the initiation stage are as follows: • Securing management support • Organizing the planning project team • Establishing the project management process • Obtaining the required resources • Developing initial project objectives	Luckey, (2009).
2. IT Business and Service Analysis	A series of assessments to identify the core IT business scenarios, IT business impacts, potential IT threats and risks, inventory of All IT systems and associated services, and resources deployed to support them.	Kadlec and Shropshire (2009); Somasekaram (2017)
2.1.IT Inventory	Identify IT inventories, such as systems, applications, hardware, data connectivity, network utilities, and infrastructure services.	Somasekaram (2017)
2.2. IT Risk Assessment	Assess the probability and impact a disaster can have on IT systems, applications, services, and hardware & software systems.	Somasekaram (2017), Acronis (2016) and Susan (2007)
2.3. IT Business Impact Analysis	Identify critical business processes and scenarios and associate them with the corresponding systems and IT assets. It is used to define appropriate Maximum Tolerable Downtime (MTD), Recovery Point Objective (RPO), and Recovery Time Objective (RTO) for each business process or a disaster	Luckey (2009; Somasekaram (2017), Acronis (2016) and Susan (2007); NIST 800-34

	scenario. RTO and RPO are associated with service level agreements (SLAs).	
2.3.1. Maximum Tolerable Downtime (MTD)	It defines the total downtime that a business can accept. MTD is always greater than or equal to RTO.	Brotherton and Dietz (2014): Somasekaram (2017)
2.3.2. Recovery Time Objective (RTO)	The total time that is required to recover an IT solution after failure.	BS ISO 22301:2012; Somasekaram (2017)
2.3.3. Recovery Point Objective (RPO)	Indicates the amount of data loss that can be accepted when a crisis occurs.	BS ISO 22301:2012; Somasekaram (2017)
3. Develop IT Recovery Strategies	Define and specify the approaches, policies, procedures and process to implement the needed resilience so as to achieve the principles of incident prevention, detection, response, recovery, and restoration.	Somasekaram (2017), Acronis (2016) and Susan (2007);Hossam (2014)
3.1.Human Aspect and Responsibilities	The teams needed to move the operations to the DR Backup Site and the Emergency Operations.	Kadlec and Shropshire (2009); Hossam (2014); Acronis (2016) and Susan (2007); NIST 800-34
3.1.1. IT Damage Assessment Team	Teams needed to assess the extent of the damage on IT operations. The team reports to the executive team, and makes a recommendation on declaring a disaster.	
3.1.2. IT Disaster Recovery Team	Works with the damage assessment team to control and coordinate recovery & backup actions, and to make recommendations to the Director of Information Services.	
3.1.3. IT Restoration Team	Manages the relocation of services and systems back to the normal.	
3.1.4. IT Site Operation team	Team assists in the recovery operations and manages the operations of the computer systems at the alternate site.	

3.1.5. IT Customer Support Team	provides assistance to customers during the disaster from the time the disaster is declared until operations resumed	
3.1.6. Communication Team	Teams that communicate during crises. Consists of a hard copy of the names and contact numbers of each employee in the departments and communication channels of main and alternate recovery personnel. Should also maintain alternate communication means such as secure lines of telecommunications during crises.	
3.2. IT DR action plan strategies	To recover critical business functions, restoration of the critical applications and critical network connectivity is the prioritization plan of the business critical functions.	Hossam (2014); Acronis (2016) and Susan (2007); BS ISO 22301:2012
3.2.1. Backup and off-site storage procedures	Procedures to backup and store at off-site location	
3.2.2. Backup Facility procedure	The offsite facility to backup to or restore from before and after crisis respectively.	
3.2.3. Emergency Response procedure	Procedure that details the basic actions that need to be taken in the event of a disaster situation	
3.2.4. Recovery Procedures	Recovery from a complete failure to a degraded mode of services.	
3.2.5. Recovery Time Table procedure	An estimated time table to recover each function and does not take into account the amount of time required to input data held on hardcopy during the recovery period.	

3.3. IT DRP Testing and evaluating strategies	Evaluating and testing strategies to return data processing activities to the primary facilities or another computer facility.	Hossam (2014); Acronis (2016) and Susan (2007); BS ISO 22301:2012; NIST 800-34
3.3.1. DRP Test procedure.	verify that the recovery procedures work as intended and that the supporting documentation is accurate and current	
3.3.2. Site Test procedures	Procedures to schedule the site tests for agreed up on day period, covering the disaster recovery procedures.	
3.3.3. Application test procedure	Procedure to ensure a site test in successfully running their applications at the alternate site including user support.	
4. Develop an ITDRP Plan	Based on the information and steps listed above, identify and prepare an ITDRP documentation of specific policies and procedures to be used in the event of a disaster	Hossam (2014); Acronis (2016) and Susan (2007); BS ISO 22301:2012; NIST 800-34
5. Conduct Test, Exercise, awareness and training	Give bi annual awareness and training once the plan has been developed. An overall testing should also be conducted per annum or quarterly as needed by the bank. Exercising after the new training and awareness is mandatory and recommended by literature.	Hossam (2014); Acronis (2016) and Susan (2007); BS ISO 22301:2012; NIST 800-34
6. Conduct Disaster Recovery Plan maintenance, exercise and Audit	Changes are inevitable, IT DRP requires continuous support and maintenance in order to fit the current requirements. Auditing the IT DRP documents, the technology and human aspects are crucial to fit to changes and preparedness.	Hossam (2014); Acronis (2016) and Susan (2007); BS ISO 22301:2012; NIST 800-34

Appendix I: Urkund Analysis Report.

URKUND

Document Information

Analyzed document	Nigussie Thesis draft.docx (D70850822)
Submitted	5/11/2020 10:10:00 PM
Submitted by	
Submitter email	nega.tarto@gmail.com
Similarity	2%
Analysis address	lemma.lessa.aauni@analysis.urkund.com

Sources included in the report

W	URL: https://www.researchgate.net/publication/228510447_Best_Practices_in_IT_Disaster_R ... Fetched: 5/11/2020 10:14:00 PM	5
W	URL: https://www.researchgate.net/publication/244478078_Evaluating_Disaster_Recovery_Pl ... Fetched: 5/11/2020 10:14:00 PM	1
W	URL: https://www.researchgate.net/publication/280841936_Development_and_Implementation_ ... Fetched: 5/11/2020 10:14:00 PM	3
W	URL: https://www.acronis.com/en-us/blog/posts/it-disaster-recovery-planning-who-should- ... Fetched: 5/11/2020 10:14:00 PM	1
W	URL: https://www.neweggbusiness.com/smartbuyer/datacenter/12-elements-disaster-recovery ... Fetched: 5/11/2020 10:14:00 PM	2
W	URL: https://www.enisa.europa.eu/publications/business-and-it-continuity-overview-and-i ... Fetched: 12/17/2019 12:11:45 AM	3
W	URL: https://mastermindsindia.com/ISCA%20SM.pdf Fetched: 10/25/2019 8:28:34 AM	1
W	URL: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technolog ... Fetched: 11/21/2019 5:45:03 PM	1
W	URL: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-stra ... Fetched: 5/11/2020 10:14:00 PM	8
J	**Implementation of it Governance Standards and Business Continuity Management in Transition Economies: The Case of Banking Sector in Croatia and Bosnia-Herzegovina** URL: 68ad1dd9-af90-499b-a6f3-9d7317bcf223 Fetched: 3/13/2019 3:10:28 AM	2
W	URL: https://docplayer.net/4407228-Business-continuity-management.html Fetched: 11/15/2019 12:05:33 PM	1