COLLEGE OF NATURAL SCIENCE SCHOOL OF INFORMATION SYSTEM

EXPLORING FACTORS AFFECTING DATA CENTER RESILIENCY: A CASE STUDY IN THE BANK OF ABYSSINIA

THIS THESIS IS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES OF ADDIS ABABA UNIVERSITY IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN AN INFORMATION SYSTEM

BY: HANA AYELE

JUNE, 2020

ADDIS ABABA, ETHIOPIA

EXPLORING FACTORS AFFECTING DATA CENTER RESILIENCY: A CASE STUDY IN THE BANK OF ABYSSINIA

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

By: Hana Ayele

Advisor: Dr. Workshet Lamnew

June 2020

Addis Ababa

EXPLORING FACTORS AFFECTING DATA CENTER RESILIENCY: A CASE STUDY IN THE BANK OF ABYSSINIA

By: Hana Ayele

Approval of Board Examiners

Advisor	Signature	Date
External Examiner	Signature	Date
Internal Examiner	Signature	Date

Declaration

I, declare that this work entitled by “Exploring Factors Affecting Data Center Resiliency: A Case Study in the Bank of Abyssinia”, is the outcome of my own effort and study and that all sources of evidences used for the study have been duly acknowledged. I have produced it independently except for the guidance of my Research Advisor.

This study has not been submitted for any degree in this university or other universities. It is offered for the partial fulfillment of Master of Science in Information Science (Information System).

Name: Hana Ayele

Signature: _____

Date: _____

Acknowledgements

First, I would to thank God, the source of knowledge and wisdom, who gives me health, power and courage to accomplish this thesis.

Next, I want to thank my advisor, Dr. Workshet Lamenew, who has shown enduring patience and guidance throughout the entirety of my study. His guidance and comments helped me in all the time of my research and writing of this thesis. And also want to thank my examiner for the probing questions that helped me to turn my initial proposal into a solid research thesis.

I am highly grateful to my husband Mr. Ashenafi Habtamu for him endured my absence when I was engaged in study and for the hours and minutes he gave me in the interstices between times of study.

I also wish to acknowledge the contributions of BOA IT staffs for taking time from busy schedule to answer some pertinent questions concerning this work.

I would also like to express my gratitude to all those who have not been mentioned in this thesis work but assisted in one or many ways to complete this thesis.

Abstract

Data center resiliency is a decisive element for banking industry. The ultimate goal of financial sector is assuring customer satisfaction by providing 24/7 services. As a result, knowing factors affecting data center resiliency is paramount importance to the financial industry.

Studies related to data center resilience show that there are attempts that treat network and storage as independent variables and such studies are very limited in number. However, a study on data center resilience needs exploration of various factors to ensure sustainable resilience. To this end, the aim of this study was to explore factors that affect data center resilience in Bank of Abyssinia taking as a case. For this purpose, a single exploratory case study approach was applied. Primary and secondary data were collected via semi-structured interview, document analysis, and direct observation. The primary data collected from technical staffs of the Bank of Abyssinia and the vendor that provides support using interview. The collected data was analyzed using Grounded theory method applying open and axial coding analysis techniques. Furthermore, the obtained factors were validated using expert judgment and cross-validating with literature results.

The study explores eight factors and unique to a single case. The major findings of study are Redundancy, Physical and virtual security, Knowledgeable Human resource, Data Center facility and site Location, communication, Top management support and commitment, Test environment and preventive maintenance and DC resiliency plan.

Because of single case study, the generalizability of the result is only for the case company. And, as this study is the first qualitative study conducted by the researcher, the amount of data collected and depth of analysis was potentially limited. So further research needs to be done for comprehensive data collection and analysis to identify factors affecting data center resiliency in the Commercial Banks of Ethiopia.

Keywords: Data Center, Resilience, Data Center Resiliency, Resiliency Factors

Table of Contents

Page

Acknowledgements i
Abstract ii
Table of Contents iii
List of Acronyms vii
CHAPTER ONE 1
INTRODUCTION 1
1.1 Research Background 1
1.2 Statement of the problem 3
1.3 Research Questions 5
1.4 Objective of the study 5
1.4.1 General objective 5
1.4.2 Specific Objectives 5
1.5 Significance of the study 6
1.6 Scope and limitation of the study 6
1.8 Structure of the Thesis 7
CHAPTER TWO 8
LITERATURE REVIEW 8
2.1 Overview 8
2.2 Data Center definition 8
2.2.1 Data Center Evolution 9
2.3 Data Center Resilience 11
2.4 Basic Components of Data Center 15
2.5 Data Center Architecture 17
2.6 Cornerstone concepts to support cyber security 18
2.7 Related works 21
CHAPTER THREE 27
RESEARCH METHODOLOGY 27
3.1 Overview 27
3.2 Research paradigm 27
3.3 Research Approach 28
3.4 Research design 28

3.4.1 Case study approach 29
3.4.2 Data Sources 30
3.4.3 Data Collection Method and Procedure 31
3.4.4 Document Review 32
3.5 Data Analysis Technique 33
CHAPTER FOUR 35
DATA PRESENTATION AND ANALYSIS 35
4.1 Background of the case Company 35
4.2 Profile of Interviewees 36
4.3 Data presentation 37
4.3.1 Data Center resiliency trend 37
4.4 Discussion 55
Discussion of result 65
CHAPTER FIVE 66
CONCLUSION AND RECOMMENDATION 66
5.1 Conclusion 66
5.2 Limitation 68
5.3 Recommendations 68
Reference 70
List Appendix 74
Appendix A: Interview questions 74

List of Tables

Table 1Summary of related works 26
Table 2 Summary of participant 36
Table 3 List of Initial Indicators and Concepts from Interviews 41
Table 4 Indicators relevant to the concept redundancy 44
Table 5 Indicators relevant to the concept Security and Threat 45
Table 6 Indicators relevant to the concept Knowledgeable Human resource 47
Table 7 Indicators relevant to the concept procedural and plan document 47
Table 8 Indicators relevant to the concept Data Center facility and site Location 49
Table 9 Indicators relevant to the concept communication 51
Table 10 Indicators relevant to the concept Top Management Support and Decision 52
Table 11 Indicators for Test environment and Preventive maintenance 53

List of Figures

Figure 1Data Center evolution phase (Alessandro2013) 10
Figure 2 Resilience capacity (Bene 2012) 13
Figure 3 Resilient versus less resilient system (Mayunga, 2007) 14
Figure 4Framework for resilient Data Center (Frincke 2016) 21
Figure 5DC-RAP (Yehia 2011) 23
Figure 6Model-building process (Saunders et al. 2009). 28
Figure 7Steps in qualitative research analysis (Fadul, 2007) 33
Figure 8Data Center resilience Assessment (Shiva, 2016) 57
Figure 9Theoretical model for factors affecting Data Center resilience 65

List of Acronyms

BoA	Bank of Abyssinia
DC	Data Centre
DC-RAP	Data Centre Resilience Assessment Portal
DoS	Denial of Service
DNS	Domain Name System
HCI	Hyper converged infrastructure
NOC	Network Operations Centre
NTP	Network Time Protocol
RAS	Reliability, Availability, and Serviceability
RWA	Routing and Wavelength Assignment
SAN	Storage Area Network
UPS	Uninterruptible Power Supplies
WDM	Wavelength Division Multiplexing

CHAPTER ONE

INTRODUCTION

This thesis explores critical factors that affect data center resiliency in the context of one of the private banks in Ethiopia, Bank of Abyissinia. This chapter gives an overview to the study and explains the structure of the thesis.

1.1 Research Background

Information systems have become significant part of our daily lives, and our dependency upon information system infrastructure is increasing. Banking services have been changed and facilitated with the use of information technology for day to day activities in order to provide quality service to their customer with the use of modern-day technology (Nada, 2018). These technologies can facilitate gathering, processing, disseminating, and storing of information in a wide range. At the core of IT infrastructure in organizations including the banking industry is the data center (Getenet, 2017).

A data center is a building (or self-contained unit within a building) used to house computing equipment such as servers along with associated components such as telecommunications, network and storage systems. It is equipped with a guaranteed power supply and high bandwidth connectivity. Among others, data centers should support continuous IT services and consequently need greater attention such as keeping them resilient. Resilience is critical, so redundancy (duplication) of networks, power and other infrastructure is common to ensure continuity. Other facilities include building management controls such as air conditioning to maintain the environmental conditions for the equipment within a specified envelope of temperature and humidity, and security systems to ensure that the facility and its data remain secure (Emma, 2013).

Data center is not a choice rather an integral part and secret of success for modern organizations. It can be considered as an area that holds, a means of hosting critical data, applications, and

servers, as well as contains basic assets of customer information, intellectual property, and other business critical data (Hailemariam, 2015).

Data center Resilience

Resilience has been defined in one of two ways, it can be defined as the ability of the system to recover rapidly from any change affecting the system routine, or as quality or state of being flexible (Hoffman and Nilchiani 2008). The main aspect of any of those definitions is to show how the performance of a system will be affected by variation of the running environment (Holling 1996). However, it is used quite differently in different fields for example computer network resilience is the ability of the network to provide and maintain acceptable level in terms of response or delay levels of services under different fault or an abnormal condition caused by cyber threats or any other threats (Mohammad 2006). In business, resilience is the ability of a company to sustain the impact of a service interruption, and resume its operations to continue to provide service (Stephanie 2019).

In defining data center "resilience" the following concepts are critical to understand (Yehia 2011):

- Operation environment: It represents the system's running condition; to quantify or evaluate the operational environment when one or more parameters are used. For example, for the system load, throughput or delay reflects the systems status (busy/ideal/abnormal).
- Threats: Each system has its own risks, either because of system vulnerabilities or because of hacker goals. For example, in a Data Center the aim of Denial of Service (DoS) is to prevent the legal users to gain access. In order to develop passive/proactive actions to build a resilient Data Center a risk assessment is required
- System efficiency: It is used to reveal the system effectiveness. If there, is a significant change in the Data Center system's efficiency, this may imply that there are malicious activities are developing and need to be investigated. We present a definition for Data Center resilience as follows: the ability of Data Center Systems to absorb any unexpected changes in the operation environment without significant changes in the Data Center efficiency and achieve speedy recovery from attacks/disturbance.

1.2 Statement of the problem

In today's financial services industry, 24/7 consistent access with the fastest transaction processing possible is required and there is simply no time for system downtime or latency (Iberahim and Mohd 2015). From trading applications that require processing in nanoseconds to credit and debit card authorizations that require transaction processing in real time, any small amount of system downtime could be the difference between financial sector, competitor, and bottom line. For achieving this 24/7 consistency, many systems and services must be available all the time. Those systems and services are connected to Data Center, so assuring the resiliency of Data Center is a critical issue for financial sector.

The information and transactions exchange within banks are sensitive and should be highly available and secure. In order to provide reliable, efficient and secure services to its customers, BOA is expected to modernize its Data Center infrastructure with resilient manner. To ensure the resiliency of a Data Center, BoA built a new Data Center with new technology; it is Hyper converged infrastructure (HCI), it combines storage, compute, and networking in one unified system, managed locally or from the cloud. With HCI, organizations can leverage the cloud's simplicity, flexibility, and scalability without losing control or compromising their ability to scale. The new Data Center design is based on spine-and-leaf network architecture, which will provide scalable, easy backup system and virtual machine mobility (https://www. bankofabyssinia.com). Building modern Data Center by itself cannot assure Data Center resiliency (Yehia, 2011).

Resilience of a Data Center (DC) is a critical element of any computer system infrastructure for a financial institution, a government agency, or a large enterprise organization. It is a complex process as it involves several aspects such as: policies for emergencies, recovery plans, variation in Data Center operational roles, hosted or processed data types and Data Center architectures (Yehia, 2011).

According to Gartner (2005), as the hub of all data and information, the Data Center must take particular care in managing and mitigating risks. In light of this, a resilience assessment as outlined here should be an essential part of the Business continuity management program of any organization that has a Data Center. Performing such a comprehensive assessment would

improve Data Center resilience and reduce risk to the organization. It would lead to improvement of Data Center site controls and add strength to the organization's overall IT resilience strategy, and provide assurance to management of the Data Center's ability to support business continuity goals.

The research conducted by Papadopoulos & Wurm (2012) identified trends, pressures, and factors that affect strategic Data Center management decisions by using case study methodology. The main intention of the researcher is identifying the trend, pressure and factors of DC Management decision regarding to environment sustainability. And they proposed Data Center resilience factors as a future work.

Bin et al. (2011) proposed a hybrid data layout policy named eStor for storage resilient for Data Center, which integrated the advantages of both sequential and random data layout policies. Under the eStor policy some replicas are placed in a sequential way, while other replicas are placed in a random fashion. It allows users to configure the system parameters of replication level and number of replicas placed in sequential way. By adjusting the system parameters, it can turn off a large amount of nodes without data loss and also has high data rebuild parallelism in case of failure. Experiments with eStor implemented in Hadoop demonstrate that it can mostly save 40% of the energy consumed and has high data rebuild rate (Bin 2011). This research views the Data Center resilience factor from the storage perspective.

Yehia (2011) proposed Data Center Resilience Assessment Portal (DC-RAP) is designed to easily integrate various operational scenarios. DC-RAP features a user friendly interface to assess the resilience in terms of performance analysis and speed recovery by collecting the following information such as, time to detect attacks, time to resist, time to fail and recovery time.

Current DC infrastructure includes many features for increased Reliability, Availability, and Serviceability (RAS) attributes; however, natural disasters threats underscore the need for a resilient Data Center (Mohamed 2011). Data Center resilience can be enhanced by improving the ability and the speed of the system to evolve and adapt to unexpected situations as they occur.

The traditional system evaluation metrics do not provide the essential information for resilience assessment.

Studies related to Data Center resilience attempted to assess treats like network, power and storage as independent variables and no concerned research could be found exploring factors in compressive manner. As literature shows, little attention was given for Data Center resilience by allegedly conducting operational, technical and managerial aspect. Data Center resilience should not be a matter of arbitrary choice these days because it has a giant importance for financial sectors.

As to the researcher knowledge, there is no research that has been done in our country to explore Data Center resilience. As a result, it was found necessary to conduct an empirical research to investigate or explore factors that affect Data Center resilience in Bank of Abyssinia in the context of Ethiopia. The nature and practices of one organization might not fit with other organization. It is therefore required to initiate this research so as to understand and fine tune the parameters affecting the resiliency of existing Data Centers.

1.3 Research Questions

The research questions this study attempts to explore and answer are the following: -

1. What are the suitable factors to consider in order to investigate Data Center resiliency?
2. How could potential improvements in Data Center resilience to be achieved in Bank of Abyssinia?

1.4 Objective of the study

1.4.1 General objective

The main objective of this study is to identify factors that affect Data Center resilience in financial sector, Bank of Abyssinia.

1.4.2 Specific Objectives

In responding to the above general objective, this research addresses the following specific objectives.

- ✓ To understand the current practice of Bank of Abyssinia to resilient the Data Center.
- ✓ To explore the factors by applying open and axial coding
- ✓ To validate the explored factors by conducting further discussion with experts.
- ✓ To give recommendation on what should be done to improve resilience of Data Center.

1.5 Significance of the study

The results of this study are significant because there was no previous research that identify factors affecting Data Center resilience and build a conceptual model for Data Center resilience. This study allows Bank of Abyssinia to consider additional, more available, cost effective and best way to improve Data Center resiliency for high level customer service and increase system efficiency and facilities because the main objective of this study is identifying the factors that affect resiliency of Data Center. Furthermore, from the collected data the researcher explore factors that affect Data Center resilience and put forward significant prepositions on how to manage these factors for assuring resilience.

Moreover, the findings may help other financial sectors to think about Data Center resilience factors in relation to the context of their organization. Besides, the result of this study can be used as an input for future studies on related topics.

1.6 Scope and limitation of the study

The scope of this study was delimited to explore factors affecting Data Center resilience and the study was conducted at Bank of Abyssinia because, since the researcher is an employee of the bank it is easy to gather information. The researcher used interview for gathering data. The data was gathered from information technology team and vendors. The reason why this research only focused on these groups is they are experienced with Data Center operation and knows better the problem, its cause and issues that should be given more emphasis.

The study is strictly limited to the available and accessible information towards the data collected from the selected case company, Bank of Abyssinia. The time limitation of this research has played a role in that. And the findings may not be generalizable to the other organizations.

Therefore, more case studies would need to be investigated in other organizations to determine whether the experience of this particular organization can be replicated to other organizations.

1.8 Structure of the Thesis

This thesis report is organized in to six main chapters.

Chapter 1: is introduction of the current study which provides background information about Data Center and Data Center resiliency, Statement of the problem, objectives, significance and scope of the study.

Chapter 2: covers literature from different sources that support the work of the researcher. It covers main topics like Data Center, Data Center evolution, resiliency, Data Center resiliency, components of reliable Data Center, and related research works towards improving Data Center resiliency.

Chapter 3: is generally about methodology followed by the study. Like research design, sampling technique, data collection instruments, procedures etc. The researcher started by describing case study research methodology as the appropriate methodology for identify factors.

Chapter 4: presents results and discussion: which defines the results after data is collected from the respected bodies and verified. It is also about analysis and interpretation of the interviewed answer.

Chapter 5: is the last chapter which provides concluding remarks of the research result and giving direction for future work.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

This chapter presents the literature review that has been carried out during the research. In order to build up the research framework, and before embarking further into the research, a literature review has been done to provide a well-grounded and thorough foundation required to carry out substantial and useful research (Boote & Beile, 2006).

Moreover, the literature review aims to provide the intellectual context the work is set in and to show the ability to navigate and evaluate work already carried out in the field. This includes the identification of opposing views, relevant methods, and people that are working in the same area. Furthermore, the aim is set at preventing the researcher from reinventing the wheel, and to identify gaps that exist in the literature. In addition, the aim is to reveal areas of possible further research, **a**nd to being able to close the identified gaps by carrying out the research. (Bruce, 1990).

2.2 Data Center definition

The main object of this study is related to Data Center resiliency and relevant factors that influence the resilient Data Center. According to Arregoces & Mauricio, (2004), "Data Center" is defined and set into a context with its overall environment. As pointed out in the introduction, the rise in the amount of Data Centers in recent years has been significant and structures that assemble Data Centers can be found throughout organizations and industries all over the world. Depending on what type of literature one reads, the definition of a Data Center can vary depending on the perspective and background from which a Data Center facility is looked at. Coming from a technical background of literature published by Cisco Press with the aim to provide information about Data Center technologies a definition of a Data Center is (Arregoces & Mauricio, 2004).

According to Mauricio (2004), Data Center is defined as, "a house for critical computing resources in controlled environments and under centralized management, which enables

enterprises to operate around the clock or according to their business needs". These computing resources include mainframes; storage subsystems; and the network infrastructure, whether IP or storage-area network (SAN). Additionally, a number of servers such as web and application servers; file and print servers; messaging servers support network operations and network-based applications, application software and the operating systems that run them. Network operation applications include Network Time Protocol (NTP) and Domain Name System (DNS).

This provides an extensive definition of a Data Center in terms of its requirements for technical capabilities and also provides a minor link to the fact that a Data Center is a structure that exists not for the purpose to solely exist, but to support an organization that operates using the services provided by a Data Center (Anixter, 2012).

Data Center (DC) is the facility used for housing a large number of computers, the servers themselves, data storages devices, and communications equipment. Data Centers are required to support critical business applications by providing the highest level of data availability, integrity, and data consistency economically feasible. Another aspect of Data Center performance is real time data backup and recovery process, Real-time backup allows Data Center mangers to duplicate their files, directories or volumes without interrupting the work which makes real time backup a better solution for business that cannot effort to have their data systems interrupted or shutdown. Traditionally Data Center mangers rely on different techniques to keep the Data Centers continually working and avoid any unexpected downtime using redundant hardware, local and remote backup sites (Maurizio, 2013).

2.2.1 Data Center Evolution

According to Stuart **(**2014**),** the concept of "Data Centers" has been around since the late 1950s when American Airlines and IBM partnered to create a passenger reservations system offered by Sabre, automating one of its key business areas. The idea of a data processing system that could create and manage airline seat reservations and instantly make that data available electronically to any agent at any location became a reality in 1960, opening the door to enterprise-scale Data Centers. Since then, physical and technological changes in computing and data storage technologies have led us down a winding road to where we are today. Figure 1 shows briefly the

evolution of the Data Center, from the mainframe of yesterday, to today's cloud-centric evolution, and some impacts they've had on IT decision-making.

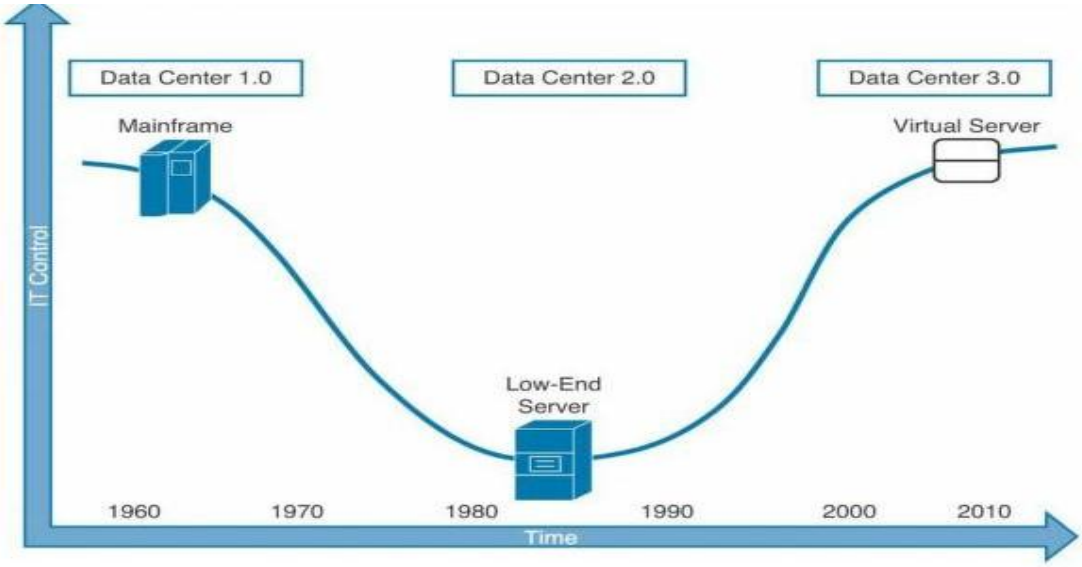

Figure 1Data Center evolution phase (Alessandro2013)

Data Center 1.0 phase name an artistic license‖ because these facilities were simply known as computer rooms then. Large and special installations, these rooms supported mainframe systems since the 1950s and, consequently, were usually designed by IBM and other manufacturers to better accommodate their central processing units (CPU) and peripherals (storage devices, terminals, printers, among others). Based on a monolithic software architecture, these centralized systems allowed a tighter control from an IT perspective and, with that, a higher resource utilization.

The Data Center 2.0, began to take shape as the client-server application model increased its adoption in the 1980s. Leveraging the popularity of personal computers (PC), application environments started a migration from mainframes to smaller ―server‖ platforms that were accessed through client applications installed on PCs. With low costs of computer hardware and the scarce bandwidth of wide-area network (WAN) links, servers in this phase were commonly deployed closer to the clients and, consequently, away from the centralized IT management. Therefore, this phase was first characterized with a multitude of low-end servers accommodated into distributed, and sometimes improvised, Data Centers. With the Internet boom in the 1990s,

computer power was once again compelled to be concentrated into Internet Data Centers, which were sometimes adapted from deactivate mainframe computer rooms. The development of internetworking and web-based applications generated a perfect storm that further increased server centralization into properly designed Data Centers. In the name of performance predictability and software modularization, the client-server model evolved to include application tiers, where each tier embodied dedicated servers that were deployed to execute specific functions. The best-known example of a tiered application architecture is the three-tier, which includes presentation, application (or business logic), and database servers.

The Data Center 3.0 phase, shares its origins with the exposed limitations of these facilities. Around the turn of the century, Data Centers were continuously approaching space and power saturation, while expansions and new facilities were the obvious expensive solutions. This phase is better characterized with a series of Data Center transformation projects that intended to improve resource utilization and increase operational simplicity. Most of these initiatives consisted of infrastructure consolidation projects, which standardized and reduced the number of components, processes, and even facilities in a corporation.

2.3 Data Center Resilience

Researchers define and describe resilience by several ways. According to Bruneau (2003). Resiliency has been defined as the ability of a system to reduce the chances of a shock, to absorb such a shock if it occurs (abrupt reduction of performance) and to recover quickly from a shock (re-establish normal performance).

Michel and Andrei (2012) define resilience by setting some requirements; a resilient system is one that shows the following characteristics:

- Reduced failure probabilities,
- Reduced consequences from failures, in terms of lives lost, damage, and negative economic and social consequences, and
- Reduced time to recovery, i.e. restoration of a specific system or set of systems to their "normal" level of functional performance.

Resiliency can be defined as the ability of the system to recover rapidly from any change affecting the system routine, or as quality or state of being flexible (Hoffman and Nilchiani 2008). The main aspect of any of those definitions is to show how the performance of a system will be affected by variation of the running environment (Holling 1996). However, it is used quite differently in different contexts; for example: in computer network, resilience is the ability of the network to provide and maintain acceptable level in terms of response or delay levels of services under different fault or an abnormal condition caused by cyber threats or any other threats (Mohammad, Hutchison and Sterbenz 2006).

In Human, resilience as the "self-righting tendencies" of the person, "both the capacity to be bent without breaking and the capacity, once bent, to spring back" (Goldstein, 1997, p. 30).

Since resilience definition by Hoffman and Nilchiani (2008), evaluation considers the system ability to continue providing services while it has been hacked or attacked. The evaluation process will identify set elements or parameters, which can be used to build a resilient and better system.

Resilience, stemming from the root, resilio, meaning to leap or spring back, is concerned with the ability of a system to recover and, in some cases, transform from adversity (Alexander, 2013).

The National Infrastructure Advisory Council (2009, 8) defines critical infrastructure resilience as: "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."

Resilience is the ability of households, communities and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty (Mitchell, 2013).

Resilience can be boosted by strengthening three different types of capacities (Bene, 2012), as shown in figure 2:

- Absorptive capacity: The ability of a system to prepare for, mitigate or prevent negative impacts, using predetermined coping responses in order to preserve and restore essential basic structures and functions.
- Adaptive capacity: The ability of a system to adjust, modify or change its characteristics and actions to moderate potential future damage and to take advantage of opportunities, so that it can continue to function without major qualitative changes in function or structural identity.
- Transformative capacity: The ability to create a fundamentally new system, so that the shock will no longer have any impact. This can be necessary when ecological, economic or social structures make the existing system untenable.

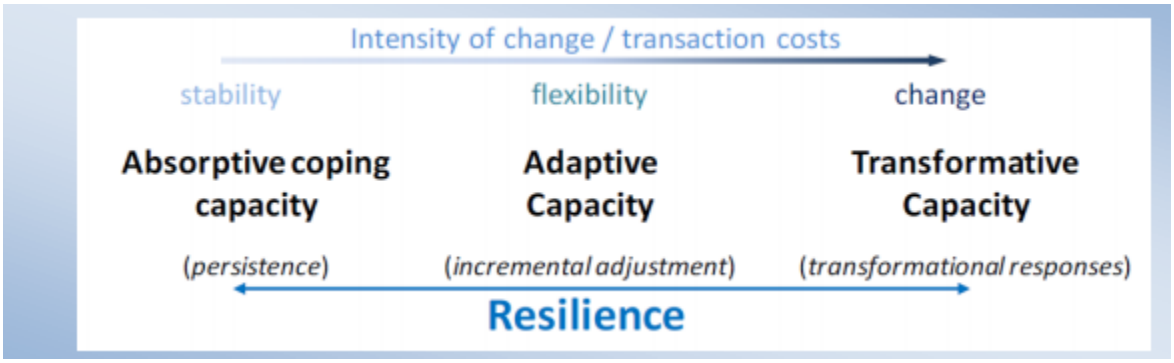

Figure 2 Resilience capacity (Bene 2012)

Data Center Resilience (or Resiliency), as described by *TechTarget* (2017), is defined as: "The ability of a server, network, storage system, or an entire Data Center, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption."

Resilience approaches emphasize the idea that disruptive events occur regularly and that systems should be designed to bounce back quicker and stronger because the impact was less. Figure 3 provides an illustration of this idea:

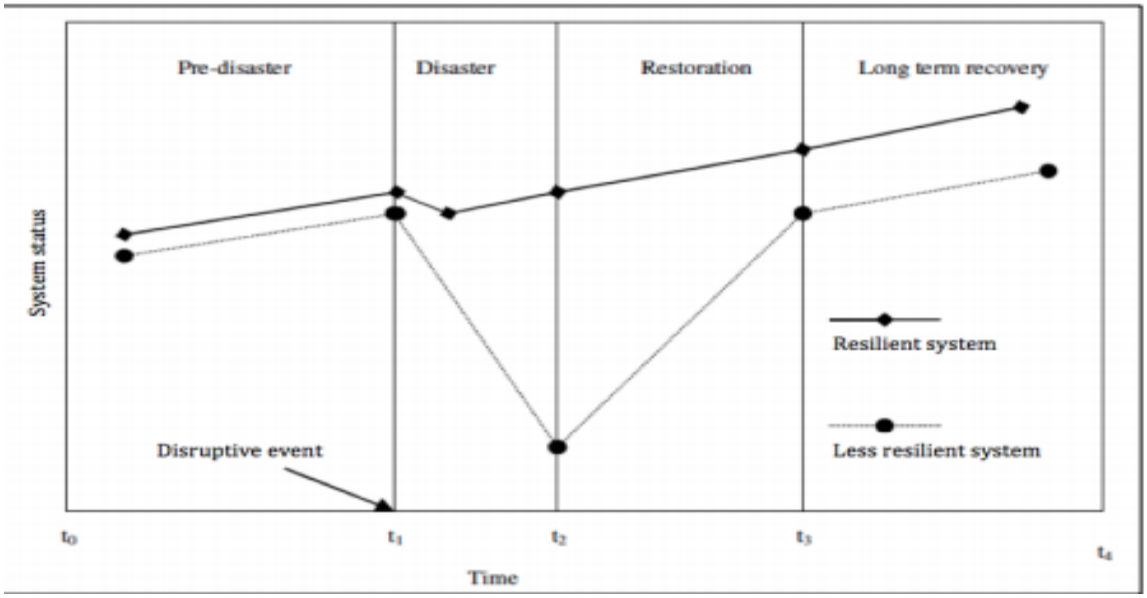

Figure 3 Resilient versus less resilient system (Mayunga, 2007)

Figure 3 above shows the more resilient system is better able to withstand the disruptive event compared to the less resilient system. In the power grid, when a shock hits, the impact is smaller (maybe part of the grid is knocked out, or there is brown outs) and the recovery is faster (full service is restored). This suggests the idea that there is a flexible continuum between functional and failed, so moves beyond the rigid duality promoted by reliability.

Data Centers need to capitalize on the real opportunity available to maximize their system reliability for continuous operations by moving toward an integrated and holistic technology approach. The foundation is a centralized, scalable, and open platform built that enables integration and interoperability providing a single, yet comprehensive view of the facility. High availability redundant control, combined with a set of critical software capabilities, allows Data Center users to precisely monitor and control all critical systems; understand cross-functional synergies, constraints, and performance and cost metrics; and immediately respond to critical events with corrective action. By implementing the right mix of enabling technologies that provide critical capabilities, Data Centers can position themselves to attain the highest level of reliability, availability, and operational efficiency optimizing the management of their facility for a sustainable competitive advantage (Halperin & Krishnamurthy 2013).

2.4 Basic Components of Data Center

According to Jonathan (2013), Data Center is typically a large, spacious facility located either, in a dedicated building (also referred to as a "server farm") or leased space within an office. Slices of space are leased to the Data Center's customers, who are responsible for moving their equipment into the facility, setting it up on racks or in cages, and connecting it to (usually backbone) networks provided by the facility.

Most facilities of a Data Center are comprised of the following components (Jonathan 2013):

- ✓ Telecommunications equipment for network connectivity
- ✓ Racks for mounting of customer equipment with overhead conduits for cables
- ✓ Cages or cabinets to physically isolate systems
- ✓ A raised floor for air conditioning, power, conduits, and flood prevention
- ✓ A fire control system and crash-and-hold bars on all doors
- ✓ An authentication system for entrance and exit; this may include a card reader, biometric device, or manned security post.
- ✓ Security cameras to view an overall state of the facility

Most facilities are unmanned and remotely managed from a network operations center (NOC). This NOC may be located in an adjacent room, on a different floor, or in a nearby building. The NOC is usually responsible for the electrical and environmental state of the entire facility including its network and hosted equipment

According to Balodis & Opmane (2014), computing facilities is a kernel of Data Center and other conditions that were adjusted. The following services are up-to-date Data Center services, such as electric supply system, environmental control, raised floor, low voltage cable routing and fire protection.

2.4.1 Electric supply system

Two aspects of energy use are critical for Data Centers (Jonathan 2013). Firstly, both IT equipment and all supporting equipment are very energy consuming. Some Data Centers facilities have power densities that exceed more than 100 times than in typical office use. For

higher power density facilities, electricity costs are a dominant operating expense and account for over 10% of the total cost of Data Center ownership.

Secondly, it is not less important to have guaranteed energy for IT equipment and also for other equipment like cooling, or access control systems used in the Data Center. Backup power systems consist of one or more uninterruptible power supplies (UPS) and/or diesel generators. To prevent single points of failure, all elements of the electrical systems, including backup systems, are typically fully duplicated, and computing facilities are connected to both power feeds.

2.4.2 Low voltage cable routing

Communications in Data Centers today are most often based on networks running Internet protocols and special protocols such as Border gateway protocol, OSPF for computing equipment interconnection. Data Centers contain a set of ports, routers and switches that transport traffic between Data Centers computing equipment and the outside world. Redundancy of the Internet connection is often provided by using two or more upstream Internet service providers (Jonathan 2013).

2.4.3 Raised floor

Data Centers typically have raised flooring made up of 60 cm removable square tiles. The trend is towards 80–100 cm void to cater for better and uniform air distribution. These provide a plenum for air to circulate below the floor, as part of the air conditioning system, as well as providing space for power cabling.

2.4.4 Environmental control

The requisite physical environment for a Data Center is rigorously controlled. Air conditioning is used to control the temperature and humidity in the Data Center. The temperature in a Data Center will naturally rise because electrical power used heats the air. Unless the heat is removed, the ambient temperature will rise, resulting in electronic equipment malfunction. By controlling the air temperature, the server components at the board level are kept within the manufacturer‘s specified temperature/humidity range the range is between 40% and 60% rH..

2.4.5 Fire protection

Data Centers feature fire protection systems, including passive and active design elements, as well as implementation of fire prevention programs in operations (Jonathan 2013). Smoke detectors are usually installed to provide early warning of a developing fire by detecting particles generated by smouldering components prior to the development of flame. This allows investigation, interruption of power, and manual fire suppression using hand held fire extinguishers before the fire grows to a large size. A fire sprinkler system is often provided to control a full scale fire if it develops. Fire sprinklers require 46 cm of clearance (free of cable trays, etc.) below the sprinklers. Clean agent fire suppression gaseous systems are sometimes installed to suppress a fire earlier than the fire sprinkler system.

2.4.6 Security

In addition to system security, Physical security also plays a large role in Data Centers (David 2016). Physical access to the site is usually restricted to selected personnel, with controls including bollards and mantraps.

Surveillance and permanent security guards are almost always present if the Data Center is large or contains sensitive information on any of the systems within. Nowadays the use of fingerprint recognition mantraps is starting to be a common place.

2.5 Data Center Architecture

According to International Telecommunications Infrastructure Standard for Data Centers the following categories are listed (*Shapiro 2015).*

TIER 1 CATEGORY: "The simplest infrastructure».

Commonly such DC has no reservation of equipment, current-carrying and cold-supplying paths. Level of service availability is about 99.67% that assumes service interruption for no less than 28 hours annually (*Shapiro 2015).* Most operations with DC infrastructure assume either partial or full cut-off of server equipment. Risk for unplanned equipment cut-off is extremely high due to technological design and a number of works on engineering infrastructure maintenance.

TIER 2 CATEGORY: Infrastructure with separate component reservation

Engineering infrastructure equipment of such DC has reservation of power and cold supply system components. Pathways (cable lines, bus wires, cold supply pipelines, copper/optical lines) aren't reserved for supply of required capacity. Basic advantage of Tier II infrastructure is the possibility of equipment item cut-off for maintenance without service delivery violation (power supply, cold supply etc.). Such DC includes requirements for security system and guard personnel. Level of service availability is about 99.75% or 22 hours of planned and unplanned break annually (*Shapiro 2015)*.

TIER 3 CATEGORY: Infrastructure with competitive maintenance

It means that each engineering infrastructure component of such DC might be taken for maintenance without cut-off of server equipment. This is the key possibility for DCs of this category. All components have N+1 reservation; pathways are designed with the possibility of «hot» maintenance using reserve lines. All server equipment shall have reservation of supply units to maintain power supply circuit by one of the lines. Level of service availability is about 99.98% or 1.6 hour of unplanned break annually (*Shapiro 2015)*.

TIER 4 CATEGORY: Defect-tolerant architecture

Architecture and technological design, rules for maintenance of such facility assume that violation of server equipment performance is possible only in case of intended act, fire, and intersection of a number of technical failures. The requirement of this DC category is duplication of all DC systems without cut-off of working load. Level of service availability is about 99.99% or 0.8 hours of unplanned break annually (*Shapiro 2015)*.

2.6 Cornerstone concepts to support cyber security

In cyber security, the acknowledged wisdom is that there is no "perfect defence" to prevent a successful cyber-attack. Frincke (2016) defined four cornerstone concepts for designing effective cyber security practices:

- Predictive Defence through the use of models, simulations, and behaviour analyses to better understand potential threats
- Adaptive Systems that support a scalable, self-defending infrastructure
- Trustworthy Engineering that acknowledges the risks of "weakest links" in complex architecture, the challenges of conflicting stakeholder goals, and the process requirements of sequential build outs
- Cyber Analytics to provide advanced insights and support for iterative improvement

In this framework, the four cornerstones operate interactively to support a cybersecurity fabric that can address the continuously changing face of cyber threats in today's world.

To provide an exceptional starting point for planning a resilient Data Center environment, especially with current generation hybrid architectures. Historically, the IT community has looked at Data Center reliability through the lens of preventive defend in the Data Center, often measured through parameters like 2N, 2N+1 redundancy (Frincke, 2016).

However, as the definition of the Data Center expands beyond the scope of internally managed hardware/software into the integration of modular platforms and cloud services, simple redundancy calculations become only one factor in defining resilience. In this world, according to Frincke's (2016), four-part framework (see figure 4) provides a valuable starting point for defining a more comprehensive approach to resilience in the modern Data Center. Let's look at how these principles can be applied.

Predictive Defence: The starting point for any resilient architecture is comprehensive planning that incorporates modelling (including spatial, and network traffic) and dynamic utilization simulations for both current and future growth projections to help visualize operations before initiating a project. Current generation software supports extremely rich exploration of Data Center dynamics to minimize future risks and operational limitations.

Adaptive Systems: Recently, Netflix has earned recognition for its novel use of resilience tools for testing the company's ability to survive failures and operating abnormalities. The company's Simian Army, consisting of services (monkeys) that unleash failures on their systems to test how adaptive their environment actually is. These tools, including Chaos Monkey, Janitor Monkey

and Conformity Monkey, demonstrate the importance of adaptively in a world where no team can accurately predict all possible occurrences, and where unanticipated consequence of a failure anywhere in a complex network of hardware fabrics can lead to cascading failures. The Data Center community needs to challenge itself to find similar means for testing adaptively in modern hybrid architectures if it is to rise to the challenge of ultra-reliability as current scale.

Trustworthy Engineering: Another hallmark of cyber security is the understanding that the greatest threats often lie inside the enterprise with disgruntled employees, or simply as a result of human error. Similarly, in modern Data Center design, tracking a careful path that iteratively builds out the environment while checking off compliance benchmarks and 'trustworthiness' at each decision point, becomes a critical step in avoiding the creation of a hybrid house-of-cards.

Analytics: With Data Center infrastructure management (DCIM) tools becoming more sophisticated, and with advancing integration between facilities measurement and IT systems measurement platforms, the availability of robust data for informing ongoing decision-making in the Data Center is now possible. No longer is resilient Data Center architecture just about the building and infrastructure. So, operating by 'feel' or 'experience' is inadequate. Big data now really must be part of the Data Center management protocol.

By leveraging these four cornerstone concepts, IT management can begin to frame a more complete, and by extension, robust plan for resiliency when developing Data Center architectures that bridge the wide array of deployment options in use today. This introduction provides a starting point for ways to use the framework, and needs further exploration by Data Center teams from various industries will create a richer pool of data and ideas that can advance the process for all teams.

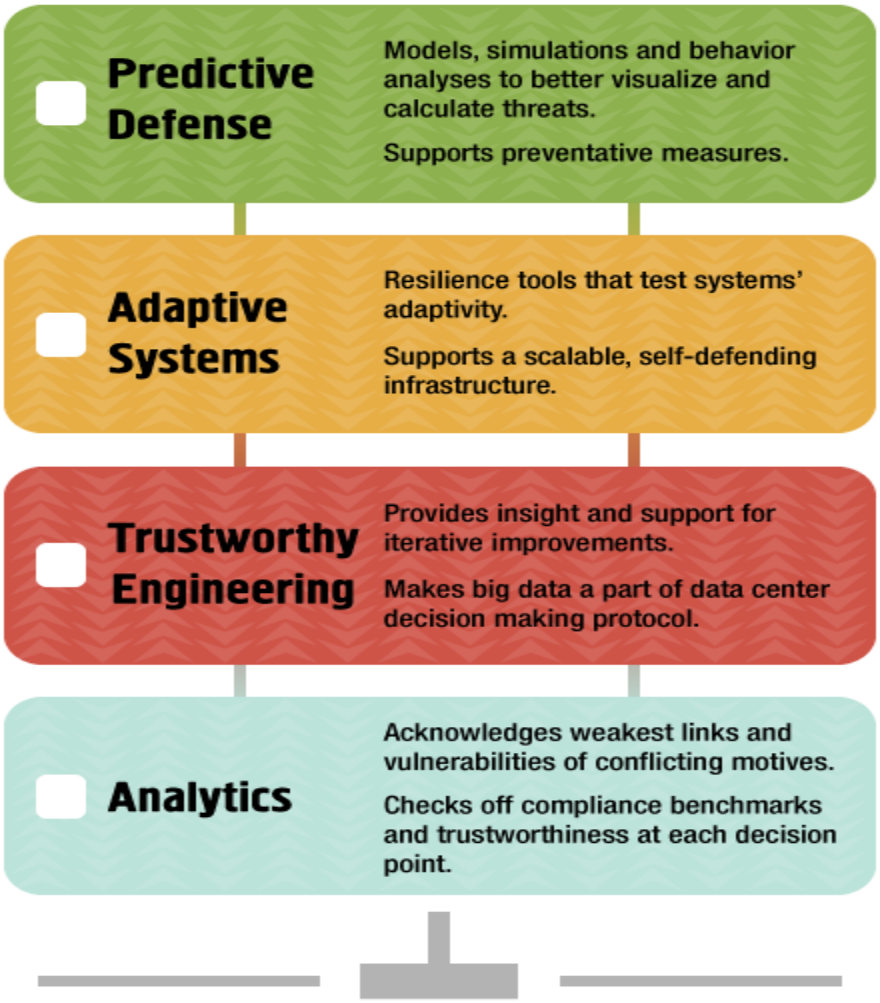

Figure 4 Framework for resilient Data Center (Frincke 2016)

2.7 Related works

In this section the researcher tries to present previous works done on Data Center resilience. Various works were reviewed from related literatures written by different scholars at different periods around the globe. These works are presented as follows:

Yehia (2011) conducted a research to study Data Center resiliency assessment and present a new methodology for Data Center resilience assessment, this methodology consists of:

- Define Data Center resilience requirements for reliability, availability, and serviceability (RAS) measures.

- Design and develop a tool. The researcher implemented a Data Center Resilience Assessment Portal (DC-RAP) for resilience evaluations.

Experiments were performed, results obtained from investigating the impact of routing protocols, server load balancing algorithms on network resilience, showed that using particular routing protocol or server load balancing algorithm can enhance network resilience level in terms of minimizing the downtime and ensure speed recovery.

As presented in figure 5, the core elements of DC-RAP include traffic generator, response time monitor, controller and logger.

• Traffic generator

It is designed to emulate accurate client/server activities; either to develop Stress tests for servers using various data loads or develops consistent traffic to setup servers for other testing purposes.

• Response Time Monitor

It measures the time interval between sending the query by the traffic generator and receiving response from the targeted server.

• Controller

This component makes the decision of directing traffic to the desired sever either manually as user preference or based on the timeout policy used. In this setting, the controller is set - automatic mode- to direct traffic to the alternative site in case of the complete failure the main site.

• Logger

This object is used to log events such as start connection, redirect traffic and other events as needed by user.

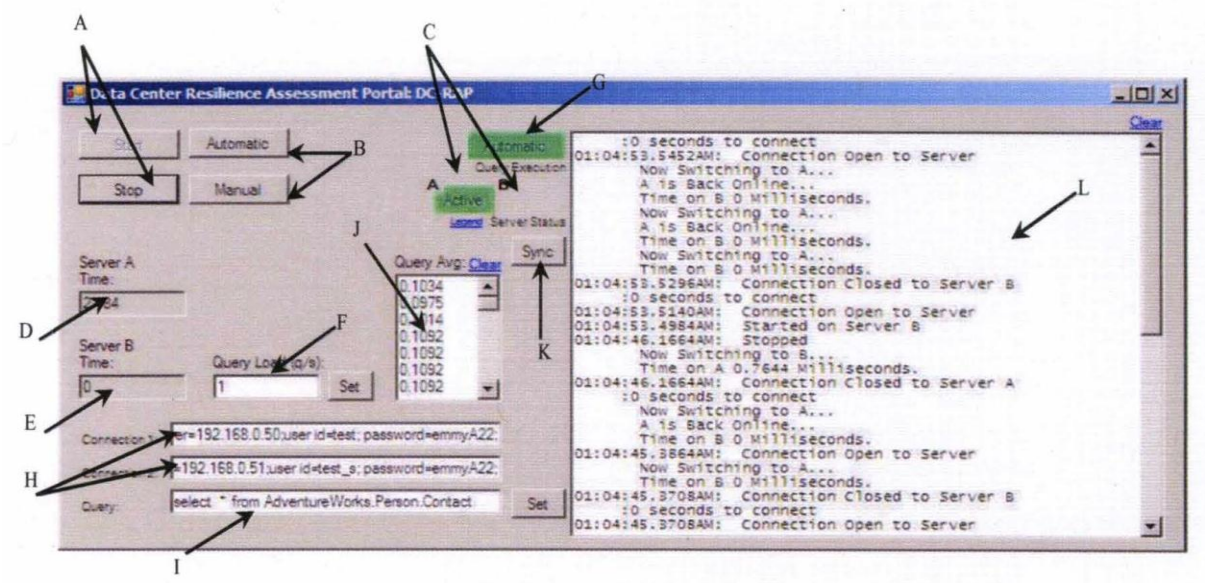

Figure 5DC-RAP (Yehia 2011)

DC-RAP

As shown in figure 5, the user interface elements are described as follows:

A. Used to start and stop the portal.

B. Automatic/Manual: use to switch operation modes to develop different scenarios.

C. Indicate the status of each server: Active, Down, and Ready

D. Total time first server was available for clients

E. Total time second server was available for clients

F. Used to set the number of query/sec

G. Indicate operation mode: Manual or Automatic switching

H. Used to setup connections: Server IPs, User Names, and Password

I. Setup the query using SQL based on applications history

J. Log of response time

K. Used to add time stamp of external actions to the log files

L. Log window

But, the developed resiliency evaluation portal shows the operational perspective of a Data Center resiliency and use design science approach so it is better to study by using other research

methodology to view other insight. The research is study on other country so it is acceptable to study in our context.

Research by Sev (2016) with the title of “Beefing up Data Center Resilience” proposes five ways Data Center operators can increase the resilience of their facility and secure smooth operations without failure by deploying the best-of-the-breed Data Center infrastructure management (DCIM) solutions. Realize Resilience Changes Constantly, have a 'Dashboard, Know Your Capacity, Run Failure Simulations and Alarms and Alerts are the main components of DCIM.

Shah (2017) attempts to design disaster-resilient Data Center Wavelength Division Multiplexing (WDM) networks. The researcher dealt with survivability of data in Data Center, when a fault occurs, is turning into an upcoming challenge in planning cloud-based applications. To deal with such a circumstance, a resilient communication code is required, so arrangements can be made to accommodate an alternative disaster-free path when a fault upsets the path utilized for data requests before the failure happens. In this work, a new approach is presented to deal with this issue, on account of the static Route and Wavelength Assignment (RWA) in Wavelength Division Multiplexing (WDM) systems. The method of utilizing multiple optical signals on a single fiber is called Wavelength Division Multiplexing (WDM). WDM in the optical system has made it possible to design large communication system with high throughput.

Routing and Wavelength Assignment (RWA): The problem of discovering a route for a light path and appointing a wavelength and resources to light paths in WDM networks is defined as the Routing and Wavelength Assignment. In their approach, a set of communication demands can be handled only if it is feasible to find:

1. the Data Center node
2. a primary light path that minimizes the effect of disasters that may disrupt light paths and
3. Every disaster that upsets the primary light path, a backup light path that handles the disaster.

This research concerns the Data Center resilience factor on the network perspective by using design science approach.

The research conducted by Papadopoulos & Wurm (2012) identified trends, pressures, and factors that affect strategic Data Center management decisions by using case study methodology. The main intention of the researcher is identifying the trend, pressure and factors of DC Management decision.

- **Trends:** The researcher identifies most important trends that were verified in the empirical data are Virtualization and Cloud Computing.
- **Pressure:** These pressures included Service Availability, Costs, Government, Laws/Regulations, SLA, Customers (internal/external), and Investors.
- **Factors:** the considered factors include Availability, Reliability, Technology, Organizational Management, Security, Customers (external) and Capacity.

Here, the study is investigating over all the Data Center factors and the researcher recommended resilience in Data Center as a future work.

Bin et al (2011) proposed a hybrid data layout policy named, eStor, which integrates the advantages of both sequential and random data layout policies. Under the eStor policy some replicas are placed in a sequential way, while other replicas are placed in a random fashion. It allows users to configure the system parameters of replication level and number of replicas placed in sequential way. By adjusting the system parameters, it can turn off a large amount of nodes without data loss and also has high data rebuild parallelism in case of failure. Experiments with eStor implemented in Hadoop demonstrate that it can mostly save 40% of the energy consumed and has high data rebuild rate. This research concerns the Data Center resilience factor on the storage perspective by using design science approach.

Summary of works related to the current research are given in table 1 below.

Table 1Summary of related works

Author (Year)	Objective of the research	Methods/ Approaches	Findings	Recommendation
Papadopoulos & Wurm (2012)	Identifying the trend, pressure and factors of DC Management	Qualitative Research	Main factors include Availability, Reliability, Technology, Security, Organizational Management, Customers (external) and Capacity	The need to identify factors of DC resilience
Yehia H. Khalil Mohamed (2011)	Assess Data Center resiliency	Design science	Reliability, availability, and serviceability (RAS) measures are the requirement of Data Center resiliency, based on which the study design and develop a tool	This study investigates resilience factor from the perspective of technical aspect. Non-technical perspective are left for future work
Umesh Shah (2017)	Design Disaster-Resilient Data Center WDM Networks	Design science	utilizing multiple optical signals on a single fibre is called Wavelength Division Multiplexing (WDM)	Propose network Data Center resilience for assuring Dc resilience other component must included
Bin Lin, Shanshan Li, Xiangke Liao, Qingbo Wu, Shazhou Yang (2011)	Design hybrid data layout policy named eStor	Experimental	Proposed a hybrid data layout policy named eStor, which integrates the advantages of both sequential and random data layout policies.	This research concerns the Data Center resilience factor on the storage perspective. Viewing Data Center resiliencies in conducive way is best for achieving the resilience

As literature shows the gap attention was merely given for Data Center resilience by allegedly conducting operational, technical and managerial aspect. Data Center resilience should not be a matter of arbitrary choice these days because it has a giant importance for financial sectors. As a result, it was found necessary to conduct an empirical research to investigate factors that affect Data Center resilience in Bank of Abyssinia in the context of Ethiopia. The nature and practices of one organization might not fit with other organization. The new research is required that help us to understand and fine-tune the parameters affecting the resiliency of existing Data Centers.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Overview

In this chapter issues related to the research approach, research design, research method, samples of the study with the selection mechanisms, instruments and procedures of data collection are presented. The chapter also discusses the research design and techniques used to answer the research questions. It covers the research paradigm, research methodology, data collection methods, data source, validity and reliability of the collected data and data analysis methods and tools.

3.2 Research paradigm

Selecting research paradigm is critical issue when conducting a study. According to Bhattacherjee (2012), research design and conduct of research is shaped by the mental models or frames of references that is used to organize reasoning and observations during the research process. These mental models or frames (belief systems) are called paradigms.

Charles & Ahmed (2017) classified Research paradigm into four categories; namely, Positivist, Interpretive, Critical and Pragmatic paradigms. Positivist paradigm defines a worldview to research, which is grounded in what is known in research methods as the scientific method of investigation. The central endeavor of the interpretive paradigm is to understand the subjective world of human experience. Critical paradigm assumes a transactional epistemology, (in which the researcher interacts with the participants). The fourth research paradigm that advocates the use of mixed methods as a pragmatic way to understand human behavior – hence Pragmatic Paradigm. Some research methodologies suited to the Interpretive Paradigm is Naturalist methodology, Narrative inquiry methodology and Case study methodology.

Thus, for the purpose of this study the researcher followed interpretive paradigm, since it is suitable to have a holistic understanding of the experience of people working in the Data Center. So Interpretive case study paradigm helped the researcher explore barriers and critical factors

that affect the Data Center resiliency and address the research questions, and ultimately achieves the research aim.

3.3 Research Approach

Broadly there are two types of research approaches, namely inductive approach and deductive approach as shown in Figure 6. In the inductive approach, the researcher collects data and develops theory as a result of the data analysis. On the other hand, in the deductive approach the researcher develops a theory or hypothesis (hypotheses), and designs a research strategy to test the hypothesis (Saunders *et al.* 2009). Induction approach gives less concern to the need for statistical generalization to population. Besides, this approach gives a chance to gain:

- understanding of the meanings humans attach to events
- Understanding of the research context through collecting and analysis of qualitative data.

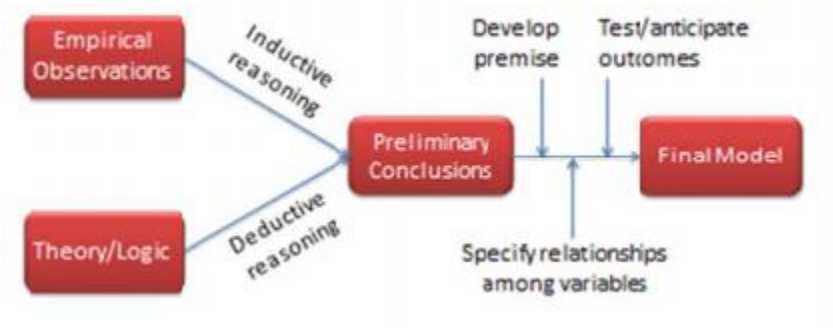

Figure 6Model-building process (Saunders et al. 2009).

Because of the purpose of the study to explore the factors of resilient Data Center experience by perception of individuals worked in Bank of Abyssinia Data Center, the research follows data analysis inductively.

3.4 Research design

According to Yin (2003), Research design is *"the logical sequence that connects the empirical data to the study's initial research questions and, ultimately, to its conclusions, and its main purpose is to avoid the situation in which the evidence doesn't address the initial research questions."*

This study follows qualitative approach. In this study several reasons make qualitative research the most suitable approach. The first reason to select qualitative approach is that there is no study conducted in our context that identifies factors that affect Data Center resiliency. Creswell (2014) emphasizes that when little is known about the research area, qualitative approach can be used to understand phenomenon. Therefore, qualitative approach is regarded to be the most suitable option for such investigation.

A researcher using interviews for qualitative research interacts, within the larger process of investigation, with that which is being investigated, with the area of study, and also with respondents. The researcher calls on reflexivity to maintain integrity a conscious process of openness to the data and commitment to see past one's biases. Though qualitative research is an exploration of values and biases and subjective experience of respondents, it is seen as valid, reliable research in its authentic adherence to the data and the perceptions of respondents. In theoretical sampling, there is an assumption of persistence that theories formulated for one group "will probably hold for other groups under the same conditions" (Glaser & Strauss, 1967, p. 49).

3.4.1 Case study approach

Case study method 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 phenomenon through detailed contextual analysis of a limited number of events or conditions, and their relationships (Zaidah 2007).

Yin (2002) defines the case study research method "as an empirical inquiry that investigates a contemporary phenomenon within its real-life context"; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.

There are several categories of case study. Yin (1984) notes three categories, namely exploratory, descriptive and explanatory case studies. Exploratory case studies set to explore any phenomenon in the data which serves as a point of interest to the researcher. For instance, a

researcher conducting an exploratory case study may ask general questions; these general questions are meant to open up the door for further examination of the phenomenon observed.

Second, descriptive case studies set to describe the natural phenomena which occur within the data in question, for instance, what different strategies are used by a reader and how the reader use them. The goal set by the researcher is to describe the data as they occur.

Third, explanatory case studies examine the data closely both at a surface and deep level in order to explain the phenomena in the data.

To explore factors affecting Data Center resiliency, this research follows exploratory case study.

On the other hand, it was important to define the unit of analysis (and therefore of the case) in relation to the way the initial research questions had been defined. The unit of analysis defines what the case is, such as an event, a process, an individual, a group or an organization (Yin 2003). Therefore, based on the research questions of the study, resiliency of BOA Data Center is defined in this study as the unit of analysis. Single case with a holistic unit (single unit of analysis) case study design was employed, and the case company was BOA.

Most case research studies tend to be interpretive in nature. Interpretive case research is an inductive technique where evidence collected from one or more case sites is systematically analyzed and synthesized to allow concepts and patterns to emerge for the purpose of building new theories or expanding existing ones (Anol, 2012). The researcher uses interpretive case research is an inductive technique.

3.4.2 Data Sources

For the purpose of this study both primary and secondary sources were used for qualitative data collection. Main sources for secondary data are the company Data Center recovery plan document, (https://www.bankofabyssinia.com/) and Data Center project documents. The secondary data retrieved from company documents were used mainly for the description of the case company. The main sources for primary data were individuals who have been working on Data Center of Bank of Abyssinia. Qualitative research data can be collected using a variety of

known techniques. The most frequently used techniques are interview and documentation (document analysis).

The selection of interviewees was purposive. Because, to collect relevant data that could help achieve the objective of the study, involving knowledgeable individuals on the subject of the study was crucial.

3.4.3 Data Collection Method and Procedure

Both primary and secondary sources were used in the study. Qualitative research Data can be collected using a variety of known techniques; the most frequently used techniques are interview, observation and documentation (document analysis).

Qualitative research provides a deeper understanding about the phenomena under deeper investigation, using tools like open interviews (Hancock et al., 2009). Primary data was collected through semi-structured interviews in order to provide the flexibility necessary to obtain valuable qualitative data, while focus on the problem and objective of research. In the semi-structured interview, the researcher has some pre-determined questions derived from the specific objectives, which can later be modified and can insert new questions during the conversation based upon the response or conversations.

Similarly, direct observation has many advantages. It is considered useful for the following reasons (Paton, 2003):

- It enables the observers understands and capture the setting within which people interact.
- It enables the observer see and understand things that people in the location pay no attention.
- It enables the observer get things that people will be reluctant to talk about in an interview.

Direct observation has also the advantage of getting the information from natural or unplanned events (Thomas 2003).

The decision on the interview design must be rooted in the research goals (Brenner, Brown & Canter 1985). The two goals in this research are to understand what factors that can affect the

resiliency of Data Center and understand the current trend of resilience in the selected case company. Above all discussion the primary aim of this thesis is to explore new factors that are perceived by the respondents so the researcher chose to adopt semi structured interview approach.

In collecting empirical data through semi structured interview, interviewees were informed about the purpose of the research and about the interview questions beforehand. This helped them to get prepared for the interview. After conducting one interview and taking notes, the process of writing complete transcript from the note was done on the same date. This helped the researcher memorize main points of the interview, and minimize loss of information. Then, before conducting the next interview the analysis of the previous interview transcript had to be completed. This had given the researcher a chance to stop the interview when the data became redundant or saturated. Following this procedure seven face-to-face interviews were conducted: As Saunders et al. (2003) noted, face-to-face interviews permit a sort of interaction between the interviewer and the interviewees.

With the presupposition that communication with one's first language is simple and useful for an in-depth discussion, the interview was conducted in Amharic. Some interviewees were willing to be audio recorded but for others after taking short notes form the interview in Amharic, the transcript was written in English. Besides, data collected by direct observation of the researcher in the form of field notes were also organized and transcribed on the same date as the observation.

3.4.4 Document Review

There are many methods of data collection usually used in case research studies. Data from two or more sources helped to support the research answers. Therefore, this study also used document review to provide a basis for extensive and thorough discussion of the research problem. The document review includes journals, conference proceedings, training manuals, videos, photos, procedure, minutes, reports, organization policy, rule and regulations, press releases and websites.

3.5 Data Analysis Technique

There are many different methods of analysis in qualitative research, the common thread is that all qualitative method of analysis is concerned primarily with textual analysis whether it's verbal or written (Patton, 2003). In this thesis, the researcher adopts one of qualitative analysing techniques/ strategy called grounded theory. It is an inductive technique of interpreting recorded data about a current phenomenon. Thus the data analysis procedure for this research followed the five basic steps of qualitative research analysis (*Kumar, 1996).* According to **Fadul (2007),** data collection, note taking, coding, memoing, sorting and writing are the basic steps in any qualitative research analysis (see figure 7 below).

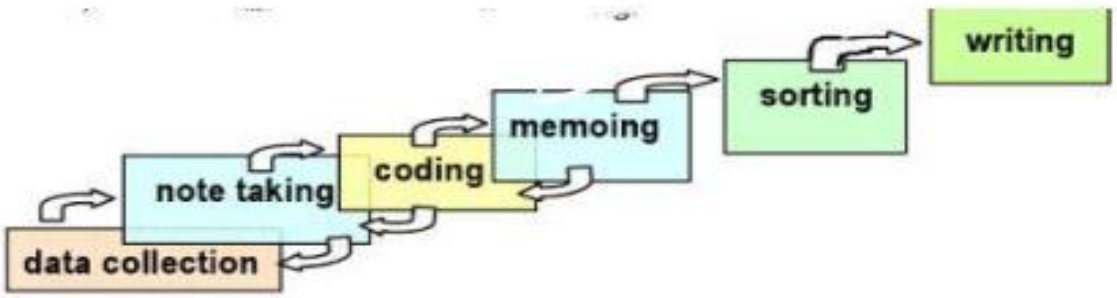

Figure 7 Steps in qualitative research analysis (Fadul, 2007)

Data collection: the researcher understands the study phenomenon through several data collection methods including interview, observation, and questionnaire. In this study primary data were gathered from selected vendor and client organizations through questionnaire and semi structured interview. Questionnaires are distributed through email address.

Note taking: After each data collection, the researcher notes down the key issues in order to get the main ideas of the results.

Coding: Categorize identical themes or relationship between themes to answer the research questions and meet the specific objectives of the study.

Memoing: write memos to yourself when you have ideas and insights and to include those memos as additional data to be analysed.

Sorting: After getting enough data, concepts were combined and arranged to explain the findings and the result of the study.

Writing: writing the final report which is guided by the above sorted data.

Data collection, note taking, and coding occur simultaneously. Sorting is done when all the above phases are saturated then writing followed at final stage.

According to Strauss and Corbin (1998) there are three types of coding open, axial, and selective. Open coding is a process aimed at identifying concepts or key ideas that are hidden within textual data, which are potentially related to the phenomenon of interest.

The researcher examines the transcribed interview data line by line to identify discrete events, incidents, ideas, actions, perceptions, and interactions of relevance that are coded as concepts called in vivo codes. Each concept is linked to specific portions of the text (coding unit) for later validation. Once a basic set of concepts are identified, these concepts can then be used to code the remainder of the data, while simultaneously looking for new concepts and refining old concepts. While coding, it is important to identify the recognizable characteristics of each concept, so that similar concepts can be grouped together later. This coding technique is called "**open**" because the researcher is open to and actively seeking new concepts relevant to the phenomenon of interest. Next, similar concepts are grouped into higher order categories. While concepts may be context-specific, categories tend to be broad and generalizable, and ultimately evolve into constructs in a grounded theory.

The second phase of grounded theory is **axial coding**, where the categories and subcategories are assembled into causal relationships or hypotheses that can tentatively explain the phenomenon of interest. Although distinct from open coding, axial coding can be performed simultaneously with open coding. At the same time, the coder must watch out for other categories that may emerge from the new data that may be related to the phenomenon of interest (open coding), which may lead to further refinement of the initial theory. Hence, open, axial, and selective coding may proceed simultaneously. Coding of new data and theory refinement continues until **theoretical saturation** is reached, i.e., when additional data does not yield any marginal change in the core categories or the relationships.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

Throughout the following chapter we will present the empirical data gathered carrying out semi-structured interviews. The presentation of the data aims to give the informed reader an insight into the findings and to further maintain and expand the chain of evidence in our research.

4.1 Background of the case Company

The present-day Bank of Abyssinia (BoA) was established on February 15, 1996 (90 years to the day after the first but defunct private bank was established in 1906 during Emperor Menelik II) in accordance with 1960 Ethiopian commercial code and the Licensing and Supervision of Banking Business Proclamation No. 84/1994. BoA started its operation with an authorized and paid up capital of Birr 50 million, and Birr 17.8 million respectively, and with only 131 shareholders (https://www.bankofabyssinia.com).

In two decades since its establishment BoA has registered a significant growth in paid up capital and total asset. It also attracted many professional staff members, valuable shareholders and large customers from all walks of life. This performance indicates public confidence in the Bank and reliability and satisfaction in its services. Currently, employing state-of-the-art banking technology, the Bank provides excellence domestic, international and special banking services to its esteemed and valuable customers. It also strives to serve all economic and services sectors via its ever increasing branch networks throughout the country. Currently the bank has more than 5825 staff and more than 309 branches and more than 1,012,177 shareholders. In addition, an authorized and paid up capital of BoA as of 30 June 2018 is Birr 4.24 billion and Birr 2.56 billion, respectively, a total deposit balance of Birr 25.9 Billion and a total loans and advances of Birr 17.99 billion, which in effect enhance the risk absorbing and the lending capacity of the Bank. Vision of Bank of Abyssinia is to be the bank of choice for customers, employees and shareholders. Its mission is to provide customer-focused financial services through competent, motivated employees and modern technology in order to maximize value to all stakeholders (https://www.bankofabyssinia.com).

Bank of Abyssinia S.C being one of the technologically rich banks in the country, has introduced many channels like SMS, Mobile banking, Agent banking, internet, ATM and POS banking services. It has been using legacy system application since its inception and is using core banking solutions since 2011 (https://www.bankofabyssinia.com).

4.2 Profile of Interviewees

The interviewees that were chosen for participation in our research are all experienced experts in their field. They have a strong connection to the Data Center operations in their organization, whether this is the core business of the organization or a service offered by the department its organization. An overview about the interviewees profile is given in Table 2.

The researcher interviewed 9 interviewee participants in a two-week period in March 2019, beginning the process of collecting indicators and open coding during and after the interview, noting concepts as they emerged in both brief notes during interviews and memos written afterward. After taking notes and writing memos, the researcher did open coding again and began comparing elements of the two interviews and noting connections between them. The shape of the interviews themselves evolved over time as concepts and meanings emerged from the data. While waiting for transcripts to come in, the researcher spent time listening to and absorbing repetitively the recordings of interviews.

The chosen interviewees were able to provide their personal knowledge and point of view about Data Center resiliency.

. ***Table 2 Summary of participants in the survey***

Position	Profession	Experience	Interview duration
Manager	Data Center	>9 years	1 hour
Manager	Network infrastructure	>12 years	40 minutes
Manager	Database	>10 years	50 minutes
Director	Vendors	>8 years	1hour
Principal	Network engineer	>7 years	35 minutes
Senior	Network engineer	>7 years	40 minutes
Admin	Data Center	>5 years	40 minutes
Admin	Disaster recovery site	>10years	50 minutes
Director	Is infrastructure	>15 years	40 minutes

4.3 Data presentation

This research study using in-depth interviews began with two questions designed to open an exploration that would identify factors regarding Data Center resilience on BoA.

These research semi-structured interviews included mainly two questions, designed to explore Data Center resilience factor. Therefore, the data presentation was organized based on the two questions accordingly.

- What Data Center resiliency practice is employed in Bank of Abyssinia?
- What are the factors that affect Data Center resiliency?

The first question regarding perceptions of trends was supplemented with sub questions asking how interviewees define the term resiliency, and what experiences they would like to see more widely distributed in the organization. The respondents had strongly agreed that, there is a clear gap in Data Center resilience and they also were eager to discuss their insights about the importance of Data Center resilience, also reflect what practices they widely used in the bank.

The second question was intended to discover factors affecting the resiliency of Data Center at BOA.

4.3.1 Data Center resiliency trend

At the beginning of each interview all participants were asked to provide their perspective and attitude regarding their understanding on resiliency of Data Center and its importance and their observation about current trend in BOA to assuring resiliency of Data Center.

According to the research participants' response, Data Center is a backbone of banking operation to serve a customer in an efficient manner. In fact, BOA are directly enabled by the capabilities of the IT and Data Center environments. So, what happens when it all fails? How much would an outage cost you? Most of all, just how resilient is your Data Center ecosystem? Those questions must be answered for assuring resilience of Data Center; so resiliency of the Data Center is the most critical issue. All respondents argued that, there is No entity who is 100% safe from some type of disaster or emergency but we can minimize the effect by building, the state of the art

Data Center to achieve resiliency using different technology. The bank tries to protect Data Center from internal and external destruction by deploying virtualization, build hyper-converged environment, build two Data Centers for main and disaster recovery site and set SLA with ISP & vendors for fast support are mentioned by research participants. These all trends of Data Center resilience on BOA Data Center are considered in this study. The evidence used to prove these concepts from participants during the interview are explained as follows.

The first interview was carried out including participant from organization. The interviewee is held with the Data Center administrator of the bank, who is also responsible for the disaster recovery site management as well. The interview was carried out using face to face interview. He made it clear during the interview that since Bank of Abyssinia Data Center resiliency and factors that are affecting Data Center resiliency. The interview has deep Data Center resiliency concept.

As mentioned by the interviewee Bank of Abyssinia is considering different trends of the Data Center because in banking sector Data Center is the backbone of business operation. So insuring resiliency of DC is the main task of organizations. Trends such as virtualization and adoption of new technology are hyper converged environment that have been mentioned during the interview. The interviewee mentioned that those two technologies maximize resiliency of the Data Center but also they have a risk of failler because of the preventive maintenance and testing of all system is not focused.

The other research participant from the vendor side said, the main trends that are ongoing and followed by the company are Virtualization. The whole Data Center effectively managed in terms of speed, reliability and security, adding new Data Center site and adopt new monitoring technology. The trend of new DC site and virtualizing it has been adopted in the last two years. This hyper-converged Data Center builds by our company and is seen as a key to drive the overall efficiency of the Data Center. Trends that are followed closely as well are Data Center monitoring technologies, those monitoring tools integrated with all critical system. As the Data Center is vertically integrated through all business processes, access to information, needed for the vast amount of applications and decisions (e.g. core system, mail system, support system,) is crucial. Therefore, many monitoring tools are used for showing alarms when storage, network

memory and CPU of those systems are under critical zone which has to be used for preventive and analysing purpose before something was happen.

The third interviewee is held with network administrator, who pointed out that, although the trends are followed on BOA, e.g. clearly identified trends that are followed and also implemented are Virtualization and build disaster recovery site. As one of the main tasks of the organization is to serve customer with speed and accurate manner because the requirements of a competitive banks must fulfils the customer needs and update themselves by technology. The interviewee said that, virtualization has the strongest impact and will be an even more important trend as technologies are still improving. The other trends are the use of web and email filtering system; so the bank staff cannot access any site or web without allowed by the organization. The other trend followed by BOA is working with disaster recovery site; the organization planning for DR site when the main site faces the problem. There after the service was continuing from this site but it is not tested, so cannot say it is fully workable.

Interviewing disaster recovery officer gave an in-depth insight about the organizations strategy towards trends. According to the interviewee there is a strong intent to discover trends early on, in order to gain competitive advantage over competitors in the market. Higher manager especially, but also other professionals that are involved in the organizations planning and development process are specially appointed to introduce new trends. These trends are then evaluated according to their possible impact in terms of beneficial outcome for the organization. However, as stated before, the organizations aim is to not end up being in this situation, but adopt feasible trends before they become requirements.

The organization strives to be able to offer solutions that incorporate the most advantageous trends to their customers. In terms of Data Centers resiliency the banks for the moment identifies all kinds of virtualization, of servers, network devices, and services as a main trend. Furthermore, energy efficiency is considered a key trend. In terms of Sustainability the connection to the organization strategy was just established recently as the organization identified sustainability as a long term goal in their vision of the choice of customer, staff and stockholders. Thus the interviewee furthermore pointed out that the organization is striving to be a role model and transport this image to their customers.

In summary, main trends mentioned by the interviewees are:

- Hyper converged Data Center
- Virtualization
- New Data Center for disaster recovery site
- Monitoring system
- Traffic filtering system

4.3.2. Factors affecting Data Center resilience

Based on the above discussion on the current trend, respondent's feedback direct that they have common understanding about the resilience practice and its importance. There are unending processes to assure Data Center resilience. However, all respondents argued that there is still a clear gap on Data Center resilience in BoA.

Each participant identified different core issues as a factor in delivering quality services, which will be discussed later in detail in the following section.

As discussed in the methodology section, this study follows the ground theory approach in order to explore the factors and construct the concepts accordingly. The ground theory approach has three consecutive phases such as open coding, axial coding and selective coding.

Initial Coding (open coding)

With each transcript, the researcher began with a process of collecting indicators—that is, words, phrases, statements from the data, or observations. In Table 3, the researcher provided an extensive list of the indicators collected from the nine interviews.

Open coding, according to Corbin and Strauss (2008) entails close examination of the data, breaking it down into parts, making comparisons, and questioning. The indicators, then, are both identified bits of data collected and data that results from the process of breaking down the data.

Table 3 List of Initial Indicators and Concepts from Interviews

▪ Data Replication ▪ Stand by device ▪ Recovery component ▪ Different Network Link ▪ Duplication of data ▪ Safety ▪ Physical Security ▪ Device Security ▪ Risk & danger ▪ Hackers ▪ Agreement with support ▪ Responsiveness of external support ▪ Communication with vendor ▪ ISP Network link availability ▪ Working together with in departments	▪ Training ▪ Inconsistent knowledge management ▪ Experience ▪ Experts ▪ Staff capacity ▪ Staff knowledge ▪ Recovery plan ▪ Procedural document ▪ Manual ▪ Guide ▪ Employee motivation & Recognition ▪ Giving Empowerment or training ▪ Management decision ▪ Prepare Conducive work environment ▪ Alarming system ▪ Alerting ▪ Service level agreement (SLA)	▪ Site Location ▪ Building status ▪ Set proper requirement ▪ Specification for Data Center ▪ Proper planning ▪ Emergency Evacuation ▪ Power ▪ Facility device ▪ Supportive device ▪ Cooling ▪ Testing ▪ Separation between production and test environment ▪ Emergency Evacuation ▪ Prevention ▪ Maintenance

The purpose of identifying the concepts was to use them to generate categories. The above list appeared to need abundant work in both grouping concepts and in breaking down concepts to allow the data to generate set of categories and be capable of containing the most important or most distributed indicators.

Axial coding (Identification of main category)

According Strauss (2007), coding process with the inclusion of axial coding as "increasingly dense conceptualization" in which linkages of categories will "eventually" lead to identification of the "core" category. Categories and subcategories are assembled into causal relationships or hypotheses that can tentatively explain the phenomenon of interest.

Categorization involves an inductive building up from the data and identifying indicators and concepts and grouping them into categories that are of greater abstraction.

As the researcher worked through axial coding, eight categories are emerged from the process which contain sub factors based on their concept similarity and relationships. The researcher shows the evolution of these eight concepts in detail.

From Concepts to Categories; From concepts and indicators, the researcher drafted a rudimentary set of 8 concepts to begin the process of analyzing and breaking down into properties:

- Redundancy
- Security and Threats
- Knowledgeable Human resource
- Procedural and plan document
- Data Center facility and site location
- Communication with support
- Top management support and Decision
- Test environment and preventive maintenance

The purpose of identifying the concepts was to use them to generate categories. The list appeared to need much work in both grouping concepts and in breaking down concepts to allow the data to categories that would be at a similar level of abstractness and be capable of containing the most important or most distributed indicators. Nonetheless, the concepts seemed to pass the tests put forward by Glaser and Strauss (1967)—that they be both analytic and sensitizing. A concept is

analytic if it is abstract enough to be analysed into properties or characteristics; it is sensitizing if it produces a picture that facilitates an understanding accessible through personal experience.

The process of analysing concepts confirmed many of the identified indicators and led to new properties as well. And another reading of the transcripts added to the list of properties and indicators. This set of concepts was characterized by some overlap and gaps that demonstrated the need for analysis and re-grouping into categories. In the following sections, I will provide a narration for the first phase of coding, for each of the 8 concepts, examining and analysing the indicators initially clustered with each concept. That process is impossible to describe or narrate with 100% accuracy since the axial coding phase actually overlapped the open coding phase. As Marshall and Rossman (1999) have said, qualitative methods are "messy".

Redundancy

Many respondents mentioned redundancy is the factor that affect Data Center resiliency. The goal of redundancy is increased reliability, which is defined as the ability to maintain operation despite the loss of use of one or more critical resources in the Data Center.

According to CISCO (2009), redundancy in Engineering can be defined as, "the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe."

Recognizing that all systems eventually fail, how you balance component vs. system-wide redundancy (N+1 vs. 2N, 2N+1, etc.) will significantly reshape the cost and benefit curve. Here, it is important to design for logical and reasonable incident forecasts while balancing mean-time-to-failure and customary mean-time-to-recover considerations.

Different respondents participated in the interview session explain about redundancy in the following way.

The vendor noted that,

"When the Data Center equipment face the faller then the operation was not continuing if there is no other standby device which replace the failed equipment.so the main Data Center equipment must be more than two or redundant".

Also the Network manager pointed out about redundancy that,

"Data Center resiliency is often achieved through the use of redundant components, subsystems, systems or facilities. Techniques, such as server clustering, support redundant workloads on multiple physical servers. From all aspect of component like network link by avail different line GPON, EPON cellular network and when we see the power if the main power is stopped then stand by generator starts automatically when the main or primary device was failed".

Further the Data Center manager explains,

"The Data Center industry has seen significant growth over the past few years as more BoA are now working with Data Center to make their businesses more agile. This translates to greater requirements around uptime, resiliency, and cost efficiency. For the most part, Data Center managers are using at least one level of duplication for power, server network and other critical component."

Analysis of the Concept of redundancy

Based on the collected data analysis, hereunder Table 4 presents summary of initial indicators relevant to the concept, Redundancy.

Table 5 Indicators of the concept redundancy

Initial Indicators	*Concept(factor)*
Data Replication Stand by device Recovery component Different Network Link Duplication of data	**Redundancy**

Security and Threat

The respondents for this research study were greatly concerned with security and generally agreed with concerning its importance as an element of resilient Data Center. In today's Data Center, strong security is an absolute prerequisite. Threats continue to morph and intensify and it is possible for a single vulnerability to imperil an organization's viability. Thus, when it comes to citizen's security (critical information), highest standards for assuring the integrity and functionality of its hosted computer base (where the critical information is stored) environment has to be maintained. As pointed out by *Data Center manager;*

"Today many bugs are release from any source which affect the internal system so protect the system from those bugs by applying different patch updates because financial factors operation is the focus area of hackers is very critical. Several security systems are combined (key card access, and separated zones for maintenance) in order to grant physical and virtual security for the company's Data Centers."

One-point network manager made was that in terms of resiliency of Data Center is the security of the data itself. This also includes the physical aspect that, depending on the customer, goes as far as from a simpler version of a locked room to a high security facility incorporating newest standards in terms of physical and virtual security, all factored together in a high security perimeter. According to *disaster recovery officer;*

"Improperly secured Data Centers are targets of hackers and worms, which can cause considerable havoc and costly damage. Internet worms and viruses proliferate in part because of inconsistent, inadequate security technologies and procedures in Data Centers. Today, known and expected threats to data cover a range of categories. Banking industry is the main focus area of hackers so proper security is needed to resilient Data Center"

The following table 5 present summary of initial indicators relevant to the concept, Security and Threat.

Table 6 Indicators relevant to the concept Security and Threat

Initial Indicators	*Concept(factor)*
Safety Physical Security Device Security Risk & danger Hackers	**Security and Threat**

Knowledgeable Human resource

The concept of Knowledgeable Human resource was mentioned by half the respondents but highly emphasized by higher management. A skilled worker is any worker who has special skill, training, knowledge, and (usually acquired) ability in their work.

According to the suggestion given by *IS director;*

"*Distributed roles among Data Center professionals and a highly skilled team that can support the overall company efficiency by resilient the Data Center if there is no skill full or capable person to manage Data Center activities or operation then the resilience of Data Center is not assured. "*

As noted further by Database manager;
"When a task moves up to manage a Data Center without proper exposure and training, when a network engineer assumes the role of Data Center ops manager, when an electrical expert takes the role of Data Center strategist or when a mechanical engineer runs a helpdesk, then "Houston, we have a problem." Many times, people grow into their positions and the new positions they assume are a far cry from their true capabilities and what they can deliver. Depending on the wrong people can prove disastrous for Data Centers. Data Centers need to be planned, implemented and ran by Data Center people, period."

Summary of indicators relevant to the concept of Knowledgeable Human resource are presented in Table 6 below.

Table 7 Indicators relevant to the concept, Knowledgeable Human resource

Initial Indicators	*Concept(factor)*
Training Inconsistent knowledge management Experience Experts Staff capacity Staff knowledge	Knowledgeable Human resource

Procedural and Plan document

The lack of concise and cohesive operation manuals, consolidated SOPs, policies and procedures, implementation of effective change control, owning and managing solid, yet simple and practical documentation can take a whole system down and prove the lack of proper documentation to be a very expensive proposition.

The document is a formal presentation created by an organization that contains detailed instructions on the plan contains strategies on minimizing the effects of a disaster, so an organization will continue to operate – or quickly resume key operations.

As pointed out by *Data Center recovery officer;*

The procedures described document have been developed to maintain a secure Data Center environment and must be followed by people working in the Data Center. It is important that any department/project contemplating the installation of their servers in the Data Center fully understand and agree to procedures.

The below Table 8 depicts summary of indicators relevant to the concept, written procedural and plan document.

Table 9 Indicators relevant to the concept procedural and plan document

Initial Indicators	*Concept(factor)*
Recovery plan Procedural document Manual Guide	Written procedural and plan document

Data Center Facility and Site Location

The site selection of a Data Center facility is being redefined as needs change due to various external factors such as higher power density, super storms, physical and cyber security, and redefined resiliency.

According to the response given by Data Center administrator,

"If the site requires an extension of high-tension power lines or requires construction of substations for distribution voltage, this can have a significant impact on initial cost and schedule. Initial meetings with the local utility company should address the availability of needed power quality and scalability of power available. Utility rate structure and incentives should also be discussed during the initial meetings with the local utility companies. Additionally, alternate power sources such as distribution generation and renewable energy need to be evaluated in the site selection process as well for corporate responsibility and incentives."

In addition, Data Center manager explains that,
"Many experienced person or management focus the computing device rather than facility device like power, cooling and related infrastructure because computing devices are available or usable for long time, the whole infrastructure must be built properly before configure and set the server and network device we should create smother infrastructure by using redundant and enough power and cooling. Many Data Centers around the world was fail manly related to power and cooling system this shows give priority to facility rather than computing and other tasks."

The site selected will have a fundamental impact on capital and operational expenditures over the life of the facility. The risk associated with a site selected without thorough due diligence can be great. The proper site selection can have a long-term positive or negative impact on the project. Therefore, it is essential that the site is scalable and incorporates the agility needed for the next-generation data centre. Determine if the Data Center is physically located in a low- to moderate-risk area, e.g., one that has a low probability of natural disasters, such as earthquakes and severe weather; access to two or more power grids for redundant power; located on high ground to minimize the threat of flooding; not close to major highways, railways or rivers.

The response of the vendor participated in the interview session explains that,
"Before build the Data Center, organization assess the location which is suitable for Data Center because Data Center need location which is free from any danger, construction area and not vulnerable for natural disaster"
Also, Data Center manager suggested as follows.
In our country most of the time there is no any assessment for site location do you remember when our Data Center the management find the wide space but not considered about is it suitable to Data Center management and emergency exit. Our country air condition is good but on other hot country the cooling area is selected in case air cooling was fail. In our experience there is no such analysis.

Summary of indicators relevant to the concept of Data Center facility and site Location is shown as follows in Table 10.

Table 11 Indicators relevant to the concept, Data Center facility and site Location

Initial Indicators	*Concept(factor)*
Site Location Building status Set proper requirement Specification for Data Center Proper planning of the DC project Emergency Evacuation Power Facility device Supportive device Cooling	Data Center facility and site Location

Communication with support

According to Sengupta, Krapfel & Pusateri, (2000), the role of communication has important implications theoretically and managerially in the services industry. Communication quality is operationally defined as the degree to which the content of the communication is received and understood by the other party in the relationship.

During the interview almost all the participants agree with, Communication is a key concept of factors mentioned in table 9. So it's considered activities such as getting support for incidents, services delivery, having proper SLA, EOL and integrity are all part of communication.

According to Kleyman (2012), when selecting the right colocation provider, creating or having a good SLA and establishing clear lines of demarcation are crucial. Many times, an SLA can be developed based on the needs of the organization and what is being hosted within the Data Center infrastructure. This means identifying key workloads, applications, servers and more. From there, an organization can develop base service agreements for uptime, issue resolution, response time and resiliency. Creating a good SLA document can take some time but it's important to do so carefully since this can govern the performance of your environment. Some very high uptime or resilient environments will build in credits into their SLA. In these situations, for example, a colocation provider could issue credits if power is unavailable. Creating an SLA is a partnership between the Data Center provider and the customer. Expectations must be clearly laid out to ensure that all performance, recovery and other expectations are met. Surprises or encountering unknowns in a production, highly utilized environment can result in loss of productivity, time and budget.

As per the comment given by the network manage concerning communication with support team;

Many times organizations will select a Data Center without actually considering the proximity to what is known as a "Response Team." Uptime within a Data Center infrastructure is always important so the proximity of the response team is very important.

Furthermore, the data base manager; mentioned that;

There are many issue which cannot be solved by internal technical staff so escalate to the external supports who is more experts on specific area the external support response must be fast and efficient. Internal staff must request support team with brief explanation.

Based on the suggestion of respondents, the below Table 12 presents indicators relevant to the concept of communication.

Table 13 Indicators relevant to the concept communication

Initial Indicators	*Concept(factor)*
Agreement with support Responsiveness of external support Communication with vendor ISP Network link availability Working together with in departments Service level agreement (SLA)	Communication with support

Top Management Support and Decision

When responding about factors, top management support and commitment was addressed by all interviewees. Network engineer statement about the importance of top management support for Data Center resilience was quoted as follows:

"Top level management is willing to accept higher costs in return for overall benefits in terms of higher initial, but lower maintenance costs, or other returns for the investment such as higher standards in order to meet pressures imposed externally without top management decision it is impossible to cover those costs so to assure resiliency of Data Center the organization should accept the cost."

In the same way, an interviewee with *principal network engineer* has also discussed the importance of top management support as follows:

If the work environment is not conducive the technical person not able to manage and monitor the Data Center operation, IT related field need more concentration and clear mind so the conducive work environment also the other factor that affect DC resiliency but prepare environment with suitable manner is the task of top management

The below table 14 shows summary of initial indicators relevant to Top Management Support and Decision.

Table 15 Indicators relevant to the concept Top Management Support and Decision

Initial Indicators	*Concept(factor)*
• Employee motivation & Recognition • Giving Empowerment or training • Management decision • Prepare Conducive work environment	Top Management Support and Decision

Test environment and Preventive maintenance

In our study the respondent strongly agree with testing and preventive maintenance is the main factors that affect the resiliency of Data Center.

The suggestion of Network manager concerning testing environment and preventive maintenance is presented below.

When designing a Data Center facility, a common mistake is failing to account for maintainability. Excess complexity can rapidly add to costs since even redundant systems must be exercised and subjected to preventive maintenance it means performing regular inspections, implementing regular updates, and proactively preventing potential failures before they occur. In fact, planning a consistent preventive maintenance schedule can be one of the most effective contributors to long-term efficiency by reducing the need for overcapacity on many key infrastructure components.

Proper testing is a necessary critical step in Data Center development. If not planned and excused with expertise, it will result in false promises and wrong beliefs in the Data Center delivery claims and abilities. People involved in the test engineering, planning, execution, supervision and

post-test report evaluation and decision-making process are key in ensuring effective tests and corrective measures to avoid serious shortages and failures over time.

Director of IT commented about the impct of testing and simulation environment in the resilence of Data Center as follows.

"When a disaster or failure happen there are many actions taken to recover with normal condition but in our country the action is the fire fighting not planned and tested before the disaster happened the action must be tested or simulated on test environment. We cannot exactly have known the impact and how much cost and time incur for resolve the issue so the resilience of Data Center affected by absence of testing and simulating. "

Also the response of Data Center Manager clearly shows the Data Center environment required for a better Data Center resiliency.

The main factors for resiliency are lack of checking alerts and properly setting alarming system. Monitoring the Data Center environment which provides the ability to quickly react to potential problems in the Data Center infrastructure and improve management. With monitoring and access, Data Center personnel have visibility into equipment operating status and receive real-time alerts and alarms to notify them of potential equipment operating problems. Remote access can also speed the response to equipment problems while real-time monitoring data can be used to populate planning tools with actual performance data.

Based on the data collected, hereunder Table 16 depicts Indicators for Test environment and Preventive maintenance.

Table 17 Indicators for Test environment and Preventive maintenance

Initial Indicators	*Concept(factor)*
Testing Separation between production and test environment Emergency Evacuation Prevention Maintenance Alarming system Alerting	Test environment and Preventive maintenance

Table 12 presents summary of the factors mentioned by the interviewees and analysed that affect Data Center resilience. The interviewees mentioned many factors in total during the interviews and summarized in to eight concepts.

Table 12 Summary of factors

Open coding	Axial coding
▪ Data Replication ▪ Stand by device ▪ Recovery component ▪ Different Network Link ▪ Duplication of data	Redundancy
▪ Safety ▪ Physical Security ▪ Device Security ▪ Risk & danger ▪ Hackers	Security and Threat
▪ Training ▪ Inconsistent knowledge management ▪ Experience ▪ Experts ▪ Staff capacity ▪ Staff knowledge	Knowledgeable Human resource
▪ Recovery plan ▪ Procedural document ▪ Manual ▪ Guide	Procedural and plan document
▪ Site Location ▪ Building status ▪ Set proper requirement ▪ Specification for Data Center ▪ Proper planning ▪ Emergency Evacuation ▪ Power ▪ Facility device ▪ Supportive device ▪ Cooling	Data Centre facility and site Location
▪ Agreement with support ▪ Responsiveness of external support ▪ Communication with vendor ▪ ISP Network link availability ▪ Working together with in departments ▪ Service level agreement (SLA)	Communication with support
▪ Employee motivation & Recognition ▪ Giving Empowerment or training ▪ Management decision ▪ Prepare Conducive work environment	Top Management Support and Decision

▪ Testing ▪ Separation between production and test environment ▪ Emergency Evacuation ▪ Prevention ▪ Maintenance ▪ Alarming system ▪ Alerting	Test environment and Preventive maintenance

4.4 Discussion

This study aims to identify the factors affecting Data Center resilience and suggest potential improvements in Data Center resilience to be achieved in Bank of Abyssinia.

The findings of this study show that the number of factors may vary depending on the Data Center type or other organizational trends. The current study attempts to review literatures with related topics and picked factors important for this study. During pilot study the researcher try to discuss with experts about the selected factors to validate the list, in which more factors were identified. The second task was to summarize factors in to 8 categories based on BOA staff and vendor viewpoint from the interview analysis results.

Redundancy

"Redundancy" is the one among the explored factors in the study. In addition to the justifications given by the interviewees about its importance the criticality of redundancy had been justified by different researchers. As noted by Jeng , Siegel & Connors, (2006), for achieving resiliency must consider redundancy: installing backup devices, such as power supplies, routers, switches and other devices that kicks in when the primary fails. Vendors tell that we need to go with full redundancy, yet it requires large investments and also is complex for monitoring or management purposes.

Therefore, selecting the critical elements to be redundant is a vital process to ensure network service continuity. Calculating the probability of system failure is one of the well-known approaches for redundancy as the more duplication the less failure probability (Connors 1984).

Recovery or resiliency from degradation state requires using alternative paths or backup devices. System designer used severe approaches to implement network redundancy.

Redundancy refers to a system design where a component is duplicated so that in the event of a component failure and IT equipment the main operation was not impacted. The main goal of redundancy is to ensure near to zero downtime.

Therefore, considering the participant's justification given in the previous section along with the other researcher support, the "Redundancy" is one of the significant factors for the organization to focus on in order to improve the Data Center resilience and ensure zero downtime.

P1*: Redundancy has a great role to improve resilience of Data Center.*

Security and Threats

During the discussion with the participant and also as the above data analysis result indicates, Security and threats are considered as a significant factor to Data Center resilience. This concept is also supported by Bernd (2010) and Frincke (2016).

Bernd (2010) defines Data Center security is the set of policies, precautions and practices adopted to avoid unauthorized access and manipulation of a Data Center resources. The Data Center houses the enterprise applications and data, hence providing a proper security system is critical. Bernd also defines Physical security is guard against physical threats such as fire, water damage, burglary and theft Protection against risks.

Frincke (2016) defined four cornerstone concepts for architecting effective cyber security practices for assuring resilience of Data Center. Such concepts include:

- Predictive Defense through use of models, simulations, and behavior analyses to better understand potential threats
- Adaptive Systems that support a scalable, self-defending infrastructure
- Trustworthy Engineering that acknowledges the risks of "weakest links" in complex architecture, the challenges of conflicting stakeholder goals, and the process requirements of sequential build outs
- Cyber Analytics to provide advanced insights and support for iterative improvement

According to Shiva, (2016), for assuring Data Center resilience, there is a need to determine what risks exist at the Data Center site that could expose the organization to a disruption. This exercise would provide a clear understanding of the risks of treats to which the Data Center site is exposed, and subsequently allows the organization to address these risks as part of its continuity program.

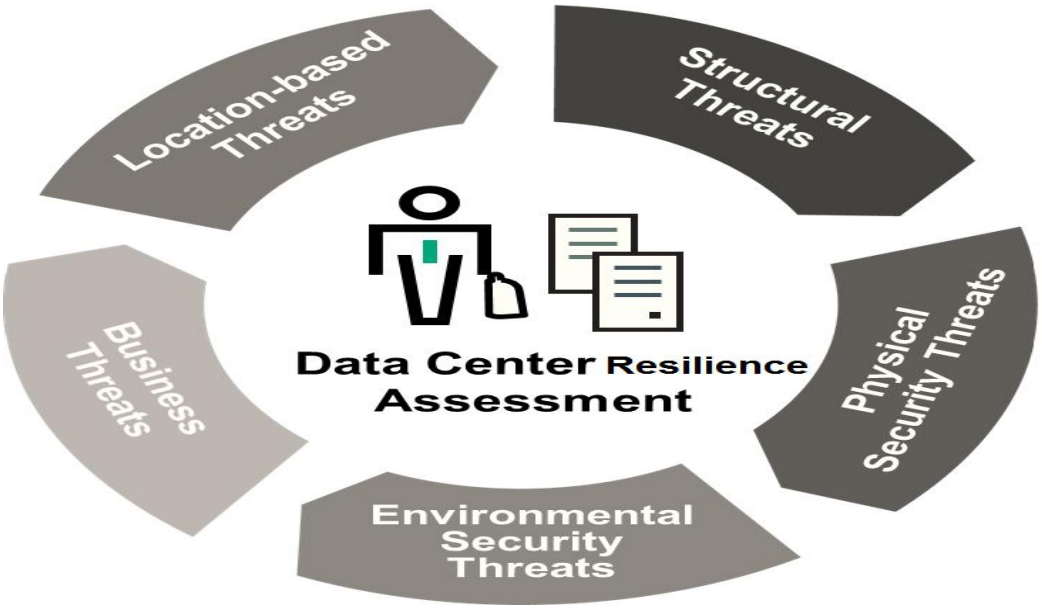

Figure 8 Data Center resilience Assessment (Shiva, 2016)

As presented in figure 8, beside location based threat, for example, climate, neighborhood, proximity to airports, military facilities, Data Center resilience assessment needs to consider the following.

- Structural threats are electricity, HVAC, gas, and water supply related threats
- Business threats such as financial, staff/knowledge, legal/regulatory
- Environmental security threats includes Smoke/fire detection, water detection, and emergency
- Physical threats considered security personnel access

Performing such a comprehensive assessment would improve Data Center resilience and reduce risk to the organization. It would lead to improvement of Data Center site controls and add

strength to the organization's overall IT resilience strategy, and provide assurance to management of the Data Center's ability to support business continuity goals. Additionally, this exercise could help prepare the organization for internal and external regulatory compliance audits.

Therefore, considering the participant's justification given in the previous section along with the other researcher support, the "Security and Threat" is the main factor the organization should focus on in order to assure the Data Center resilience.

***P2**: Security and avoiding threats has a vital role for achieving resilience of the organization Data Center.*

Knowledgeable Human resource

This study has revealed that *"Knowledgeable Human resource"* is from among the widely discussed factor of datacenter resilience in BoA. This factor had been also addressed and discussed in many of the reviewed literatures. Marty (2016) stated that due to its complex nature, a Data Center cannot operate effectively or efficiently if employees are not adequately trained. It is necessary to verify that workers have processed the material and will be able to put it into practice on the job.

All employees, regardless of their job description, should receive training on:

- Safety and emergency procedures
- Facility operating procedures
- Industry standards and best practices
- Compliance with relevant regulatory laws and government codes Based on their duty requirements and level of expertise, employees should also receive ongoing technical training similarly, and we can deduce another support for knowledgeable human resource is the main factor for Data Center resilience.

A Data Center administrator (DCA) is an experienced information technology (IT) professional who is responsible for overseeing Data Center operations. Because DCAs are in charge of business-critical systems, they need to have an in-depth knowledge about everything that occurs in the Data Center, including infrastructure design, operations and lifecycle management for physical and virtual Data Center assets (Erica 2018). DCA works on the organization must have the above skill to troubleshoot and minimize the effect of some threats for improving Data Center resilience.

Robert and Patrick (2017) revealed that, maximizing availability and minimizing human error in the critical systems environment depends, in large part, on well trained staff. A suitable training program must be established that organizes all of the operational and maintenance tasks into categories that correspond to specific levels of capability (such as, Basic, Intermediate, and Advanced). All operations and maintenance activities should be mapped to one of these levels. This provides the ability to control work assignments and ensure that, all activities are being carried out by properly qualified personnel.

Stéphane (2017) study about common case of Data Center failure, whether the staff discuss about mistakes made during design, installation or maintenance. Stephan noted that, people are often to blame for Data Center failure. The Uptime Institute cites that nearly 70% of Data Center outages can be attributed to human error. Many aspects of a Data Center invite the potential for mistakes, whether due to illogical layout, poor (or no) labeling, lack of maintenance or inadequate training. Even the simplest oversight can result in a serious downtime event that may be difficult and costly to recover from. So we must focus to have knowledgeable human resource to protect the resilience of Data Center.

As a result, to alleviate the above mentioned barriers, the researcher has a strong belief that there should be continuous capacity building to knowledgeable human resource. This implies that training and expertise of people working on Data Center is decisive for assuring datacenter resilience.

Thus, the finding of this study has confirmed the argument of Stéphane (2017) and Marty (2016,), that *"Knowledgeable Human resource"* is significant factor that affect datacenter resilience.

***P3**: Having Knowledgeable Human resource in organization is a valuable factor for improve resilience of Data Center.*

Data Center Facilities and site Location

The result of the study indicated that "*Data Center facilities and site Location*" is critical factor for Data Center resilience.

According to Rajan (2014), there are four main parameters that should be considered in the Data Center location decision: power, connectivity, cooling systems, and natural hazards.

The misalignment of Data Center facilities (power, connectivity, cooling systems, and natural hazards) in relation to the IT (network, storage, etc.) has caused too much damage and wasted too many resources as well as operational hours beyond description and Data Center sustainability. We have far breached the borders of obsolescence when still facing this traditional and unjustified misalignment in Data Centers. Unfortunately, widely practiced by people, this continues to be a visible and consistent gap across organizations.

According to Gartner (2005), location of the Data Center will greatly affect security, operational efficiency and operating costs. Site criteria should include ensuring that there is reasonable commuting distance for employees, support vendors and other constituents; sufficient site area for parking, water and fuel storage; space for delivery truck access; and a location away from high-risk areas, such as airport-approach corridors, flood plains and areas that are prone to natural disasters, such as earthquakes, tornadoes or hurricanes. Avoid collocating near potentially hazardous areas, such as cafeterias, machine shops, wet labs or other facilities where fires or machine vibrations could present a hazard to Data Center operations.

Choosing the location is an important strategic task when planning a new Data Center, as it will impact virtually every step of the planning and realisation process as well as the future operation

of the center and extension possibilities. It is not uncommon in the Data Center industry to spend significant effort and resources on finding and acquiring the optimal site for a new Data Center. It is therefore unsurprising, that the industry has written widely about the factors that ought to be considered, when selecting a future location (Ladina, 2013).

There is no site that is perfect; therefore, the above parameters should be evaluated holistically. The evaluation of each parameter should be benchmarked with a business case for each site and optimal solution for assuring Data Center resilience. Before built a Data Center the organization should consider the site and facility device for the effective and resilient optionality of the DC.

***P4**: Inaccurate selection of Data Center facilities and site has negative influence for assuring the resilience of Data Center.*

Top management support and Decision

The study revealed that top management support and decision is important factors that affect Data Center resilience in both the theoretical literature and the empirical study. When we refer to the theoretical literature, its significance was highly pronounced in Data Center resilience. With this respect, Erica (2018) stated that:

"The higher managers are responsible for appropriate layout for all equipment in the Data Center. This includes the initial implementation and setup of the Data Center (if required), the on-going retirement and addition of new hardware and an understanding of the electrical, load balancing and cooling needs of the equipment. Without those higher management support and decision achieving Data Center resilience is impossible."

An effective management must develop a wide range of technical and business skills. The scope of responsibilities for the Data Center administrator spans multiple IT disciplines and requires knowledge of hardware, software and the business' requirements for computing resources. For example, a DCA must be able to make recommendations for equipment and procedure changes to decrease costs and increase efficiency and resilience of a Data Center (Margarit 2019).

The higher managers must understand how these systems work, both independently and with each other, and feel comfortable explaining the expected benefits of a particular technology or service to stakeholders (Erica 2018).

At the enterprise level, a higher management is responsible for multiple Data Centers and negotiating service level agreements (SLAs) with multiple service providers.

This finding provides empirical evidence which supports the argument of Margarit (2019) and Erica (2018) that Top management support and decision is critical to the resilient Data Center.

P5*: Top management support and Decision has momentous impact on Data Center resilience.*

Test environment and preventive maintenance

Test environment and preventive maintenance is the core aspect of continuous service improvement. It is important factor to Data Center resilience. In both the literature and the empirical study the importance of this factor was magnified. John (2016), Thierry (2011) and Mehdi *(*2015) tried to show the importance of Test environment and preventive maintenance in relation to feedback through recording and reporting. John (2016) describe about testing it represents the only opportunity to ensure that the facility is as robust as expected: to make sure the design and construction work deals with a variety of different scenarios and maintains availability. The negative impacts of down-time can be losses in both financial terms and brand reputation. The testing phase gives the owner the safety and knowledge that the facility has been designed and built well and operates to the planned processes of design.

Thierry (2011) defines the term preventive maintenance (also known as preventative maintenance) implies the systematic inspection and detection of potential failures before they occur. PM is a broad term and involves varying approaches to problem avoidance and prevention depending upon the criticality of the Data Center.

Thus, this result confirmed the argument of the authors that stated Test environment and preventive maintenance is a factor that affects datacenter resilience.

P6: *Absence of Test environment and preventive maintenance in Data Center has negative impact on the resilience of DC.*

Procedural and Plan document

Procedural and plan document is the core aspect of continuous DC resilience improvement, which is one component of the organizational plan. It is an important factor of Data Center resilience. In both the literature and the empirical study, the importance of this factor was such magnified.

According to Shiva (2016), IT disaster recovery planning, or "IT resilience" planning as it is often termed, is typically application-driven. When a business sets out to build its IT resilience strategy, plans, and infrastructure, it typically performs a business impact analysis (BIA). The BIA identifies the most critical applications, and consequently the IT infrastructure that supports it, and builds recovery plans for them. Thus Data Center is the main critical issue of the organization.

Disaster recovery in a nutshell is data recovery and service continuity after a failure or a disaster. With disaster recovery sites companies aim to minimize the impact of disasters. To fully utilize a disaster recovery site, organizations need to establish business impact analysis on their environment along with risk analysis. Based on these impact and risk analysis, organizations can produce a working disaster recovery plan. Understanding the impact, identifying critical assets and restoring functions after a disaster, is the main goal when planning for disaster recovery (Cisco Systems, Inc. 2006).

This study revealed that because of the weakness in the preparation of Procedural and plan document in BoA Data Center resilience irregularity of activities and difficulty of maintaining momentum was prevalent.

P7*: prepared proper procedural and plan document has significant role for resilient Data Center.*

Communication with support

The result of the study indicates that communication is one of the key factors affecting the resilience of Data Center. Based on observed in the evidence found from this research result and literature the researcher understand that lack of communication is the main factor of Data Center resilience.

According to Ernest (2018), Data Center SLAs guarantee a certain level of uptime, which indicates the percentage of time their systems are available. For a modern, enterprise level Data Center, nothing less than 99.99% uptime should be considered acceptable, and even that should be considered an absolute baseline minimum. Each additional "9" offers a significant increase in reliability.

Sometimes, things go wrong. In the IT world, this tends to happen quite a lot! Data Centers need to provide assurances that their staff will be able to respond to problems quickly and effectively. If there's an issue at the facility, customers need to know that support will be available 24/7/365 to address it. Are systems monitored by onsite staff at all hours of the day? How much transparency do customers have over their IT assets? Those questions must have been answered for assuring uptime or resilience of Data Center.

Data Center staff should be available to provide all manner of support at all times. If the Data Center SLA is unclear about how much technical support is provided for migration and maintenance, customers should ask pointed questions for clarification. When a company commits to a Data Center provider, it should feel comfortable with who it can contact when problems arise and what kind of response it can expect (Roderick 2018).

Based on the above discussion the researcher takes the communication as a significant factor for Data Center resilience.

P8: Active Communication with support is a guarantee for the resilience of the Data Center.

In general, the finding of this study about factors affecting resilience of Data Center in the theoretical pattern and supported or confirmed by this study. From these findings we can realize

that almost all factors seemed to have similar effect respective of the context in which Data Center resilience. Based on the finding of the study the researcher formulates theoretical model (depicted below in figure 9) in order to show the significance of the above prepositions on the Data Center resilience.

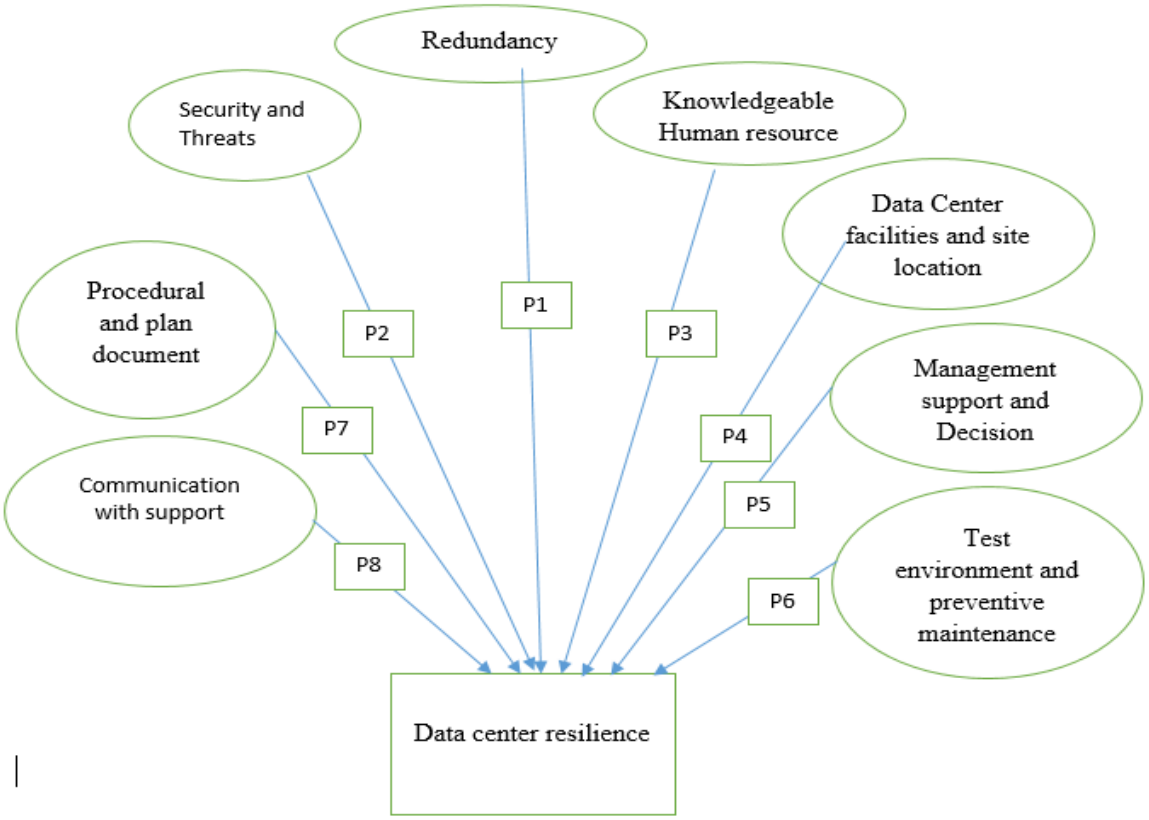

Figure 9Theoretical model for factors affecting Data Center resilience

Discussion of result

The findings and the case study analysis has been discussed well in this chapter. The result shows the Data Center resilience depends on factors, such as communication with support, procedural and plan document, Test environment and preventive maintenance, Management support and decision, data centre facilities and site location, knowledgeable human resource, security and threats and redundancy. In this regard this chapter identified the factors that affect Data Center presents the theoretical model in the context of bank of Abyssinia. Finally, this chapter presents a factor of Data Center resilience which is not used and found in any other research paper.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

This study aimed at investigating the factors for Data Center resiliency in Bank of Abyssinia so as to examine current practices or trends employed by the bank and identify the factor with it. The final part of this thesis deals with discussion of the major findings, conclusions and the recommendations which the researcher assumes to be operational are also forwarded on the basis of the findings.

5.1 Conclusion

In the financial sector providing the insight about the factor that affect business continuity is vital; thus, Data Center resilience is the crucial factor that affects business activity of the financial industry. Data Centers have the lowest tolerance for risk and therefore the greatest demand for resiliency than nearly any other type of facility. Whether for primary production, test & development or alternate site backup purposes, care should be taken to select sites that are sufficiently risk-free and protected against things like utility disruption, a local incident or a larger scale disaster. Alternate sites should be built and/or located to eliminate or mitigate risks that are in-common with the primary site, but close enough for ease of relocation. If it is a vendor/third-party site, the best fee schedule should be negotiated up front to meet business requirements, both present and projected. If it is an internal site, the infrastructure should be prepared to support the current and projected requirements and there needs to be clear ownership of responsibilities Data Center infrastructure.

A suitable alternate/back-up site can be validated by the following activities:

- Documentation of recovery requirements and the strategy to meet those requirements so that different solutions can be analyzed
- Comparison of the facility features (Data Center, work area, storage) provided at the alternate site against the strategy requirements

- Assessment of the Data Center infrastructure to confirm concurrent maintainability without costly service downtimes, along with other resiliency requirements for the facility
- Contract reviews with third party vendor selection. Examine areas such as the procedures for invoking the declaration to occupy the site, the time required between invoking and when access is actually permitted
- If the site is an internal location, a thorough understanding of who owns which responsibilities (facilities versus IT) and a review of the maintenance and test procedures required to keep the site in a state of readiness.

Incorporation of an alternate/back-up site is a cornerstone of your resiliency strategy. In the event of a disaster impacting production, business will continue and market share will be maintained.

The concept behind Data Center resilience explained in detail along with an investigation of the gap for DC resilience from the case study organization and review of literature. The data was analysed using ground theory analysis based on the data collected from case company through the semi-structured interview. Eight significant factors were explored such Redundancy, Security and Threat, Knowledgeable Human resource, procedural & plan document, Data Centre facility & site Location, communication with support, Top management support & Decision and Test environment & preventive maintenance. Those factors are evaluated by expert and different literatures and the researcher provided proposition for each factors.

P1: Redundancy has a great role to improve resilience of Data Center.

P2: Security and avoiding Threats has a vital role for achieving resilience of Data Center.

P3: Having Knowledgeable Human resource in organization is a valuable factor for improve resilience of Data Center.

P4: Inaccurate selection of Data Center facilities and site location has negative impact for assuring the resilience of Data Center.

P5: Top management support and Decision has momentous impact on Data Center resilience.

P6: Absence of Test environment and preventive maintenance in Data Center has negative impact on the resilience of DC.

P7: Prepared proper Procedural and plan document has significant role for resilient Data Center.

P8: Active Communication with support is a guarantee for the resilience of the Data Center.

5.2 Limitation

This research had several limitations that must be noted. First, because this was a single case study, the generalizability of the result is only for the case company. Second, as this study is the first qualitative study conducted by the researcher, the amount of data collected and depth of analysis was potentially limited by the experience of the researcher.

5.3 Recommendations

A study provides critical points to the selected organization in order to provide the resilience of Data Center. So, this research highly recommends a case company and other organization to give focus on the explored factor to improve their Data Center resilience.

The higher management should be aware of the existing problem on the Dc and take action or decision to provide solution for the explored factor and assign budget for enhance the knowledge of staff, security devices, for redundancies of critical components and evaluate the level of Data Center resilience by assessing and monitoring the DC operation.

Generally, BoA needs to focus its efforts and resources on factors that affect Data Center resilience to assure a competitive financial sector on the business.

5.3 Future work

The study has not been entirely conclusive and has led to many questions related to DC resilience practices of financial organizations. Further studies are therefore required to both extend this research and help improve the DC resilience practices in financial organization. Therefore, based on the conclusion to this study some future work recommendations are presented below:

- The explored factors can be tested by other researcher by using quantitative method and select the most critical factors.
- Required other study to improve the constructed theoretical model.
- Identifying Data Center resilience factors by involving participant from other organization.

Reference

Alexander, D. (2013). Resilience and disaster risk reduction: an etymological journey, University College London, London, UK

Azodolmolky, S. (2013). Software Defined Networking with Open Flow, Packt Publishing Ltd, University of Essex, UK

Bank of Abyssinia, retrieved on 20/11/2018 from https://www.Bankofabyssinia.com/Home

Bank of Abyssinia financial report of 2011/12 retrieved on 20/11/2018 from https://www.bankofabyssinia.com/annual financial report 2011/12

Bene, C. (2012). Resilience Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability-Reduction Programs, Institute for Development Studies Working Paper, Brighton Article review

Bill, K. (2012). Best Practices and Critical Considerations for Choosing the Right Data Center Colocation Solution, university of Helsinki Finland master's thesis

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices, University of South Florida Article review

Bin, L., Shanshan, L., Xiangke, L., Qingbo, W.& Shazhou, Y (2011). eStor: Energy efficient and resilient data center storage, University of Luxembourg

Boote, D. & Beile, P. (2006). Centrality of the Dissertation Literature Review in Research Preparation.

Booth, W. C., Colomb, G. G. & Williams, J. M., (2008). THE Craft OF Research. 3rd ed. Chicago: The University of Chicago

Bowen, G. A. (2009) Document Analysis as a Qualitative Research Method. Qualitative Research Journal, Vol. 9 No. 2, pp. 27-40.

Bruce, C. S. (1990). Information skills coursework for postgraduate students: investigation and response at the Queensland University of Technology. Australian Academics & Research Libraries, 21(4), pp. 224-232

Bryman, A. (2012). Social research methods. 4th ed. New York: Oxford University Press.

Cao, B., Gao, X., Chen, G. & Jin, Y., (2014) NICE: Network-aware VM consolidation scheme for energy Conservation in data centers, IEEE ICPADS, 166–173.

Charles, K. & Ahmed, B. (2017). Understanding and Applying Research Paradigms in Educational

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. SAGE Publications

Creswell, J. W. (2007). Qualitative Inquiry and Research Design - Choosing Among Five Approaches. 2nd ed.: SAGE publications

David, M., Junjie, W.& Thomas, F. (2014). Towards a Scalable Data Center-level Evaluation Methodology, University of Michigan

Ernest, S. (2018).Service Level Agreement (Sla) & Uptime of Data Center, Florida US

Fadul, J. (2007). A Workbook for a Course in General Psychology. King's College London

Flick, U. (2009). An introduction to qualitative research. 4th ed.: SAGE.

Frincke, D. (2009) "I4 Newsletter", Pacific Northwest National Laboratory, Spring-Summer.

Getenet, W. (2017) Data center virtualization framework in banking sector: the case of Wegagen bank S.C

Greenfield, T. (2002). Research Methods for Post Graduates London, Arnold, 370pp

Gustavo, A., & Andrade, S, (June, 2013) Data Center Virtualization Fundamentals, United States of America

Hancock, B., Ockleford, E. & Windridge, K. (2009). An Introduction to Qualitative Research. University of Birmingham

Henn, M., Weinstein, M. & Foard, N. (2009). A critical introduction to social research, 2nd ed., Sage Publications, London.

Hesse, B., & Leavy, P. (2011). The practice of qualitative research, 2nd ed., Sage Publications, Thousand Oaks, California.

Hoffman, J., & Nilchiani, R. Assessing Resilience in the US National Energy Infrastructure. Vancouver, BC, Canada

Holling, C.S. (1996). Engineering Resilience versus Ecological Resilience. In: Schulze, P.E., Ed., Engineering within Ecological Constraints, National Academy Press, Washington DC

Emma, F. (2013). data center publication. Retrieved February 2019 from https://www.techuk.org/insights/reports/item/html

Jack, W. (2014). The evolution of the data center : Timeline from the Mainframe to the Cloud University of La Verne Academy

Jonathan, A. Z. (2013) data center threats and vulnerabilities University Of Arizona

Kothari, C. (2004). Research Methodology: Methods and Techniques. New Age International Publishers.

Kumar, R. (1996). Research Methodology: A step by step guide for beginners, First edition

Kvale, S. (1996). Interviews - An Introduction to Qualitative Research Interviewing.: SAGE Publications.

Lee, G. (2014). Data Center Evolution—Mainframes to the Cloud Waltham, USA

Liu, V., Halperin, D., Krishnamurthy, A., & Anderson T. (2013). a fault-tolerant engineered network, university of Washington

Marshall, C. & Gretchen, B. (2006). Designing qualitative research, 4th edition, Thousand Oaks, Sage Publication, pp. 97 – 150.

Marty, M. (2016). Evidence-Based Best Practices Around Data Center Management Massachusetts Institute of Technology

Martin, E. (2018). Engineering Physics and Electrical Engineering Hopkins University

Martin, E. (2018). Monitoring, Modelling and Identification of Data Center Servers Lulea University of Technology

Nada, B. (2018). Impacts of information technology (IT) <https://master-iesc-angers.com/impacts-of-information-technology-it/ > [Viewed 06/02/2019]

Papadopoulos, C., & Wurm, A. (2012). Trends, Pressures and Factors that affect Data Center Management taking Environmental Sustainability into Account The University of Chicago.

Robert, W & Patrick, D. (2017). Essential Elements of Data Center Facility Operations, Rueil-Malmaison, France

Roderick, B. (2018). The Challenges of Opening a Data Center, Stanford University

Turner, D. W. (2010). Qualitative Interview Design, Nova South eastern University

Saul, S. (2017). Component of data center. Retrieved February 2019 from https://atfirstlight.net/key-components-of-a-data-center

Umesh, S. (2017). Design of Disaster-Resilient Data center WDM Networks University of WindsorFollow

Yehia, H. (2011). Data center resilience assessment: storage, networking and security. University of Louisville.

Yin, R. (1994). Case Study Research: Design and Methods, 2nd Edition, Sage Publications, London, UK.

Yin, R. (2003). Case Study Research: Design and Methods, 3rd. Edition, Sage Publications, London, UK.

Zaidah, Z. (2007). Case study as a research method, University Technology Malaysia.

List Appendix

Appendix A: Interview questions

This interview has been designed to gather data for the fulfilment of the thesis requirement for the degree of Master of science in Information System.

Participant in this study is voluntary.

Short general block of questions:

1. Could you please provide us some information regarding your professional background and position? a. Main area of operation

Detailed questions matching the research questions:

1. What is data center resiliency?

2.Is data center resiliency different from data center availability and disaster recovery?

If yes, how it is different?

3. Is DC resiliency considered a factor in your organization activity (Bank of Abyssinia)?

   a. If not, then why is not considered as a factor?

   b. If yes, in what way do you consider DC resiliency in your organization?

   c. If yes, which are the main benefits for your operations being resilience (e.g. cost savings/improvement of image)?

4. What are the key factors that have to be considered in a Data center resiliency?

5. What additional factors do you think are important?

6. Which of the mentioned factors are the most important ones? Factors that affect Data center resilience?

7. Do you think that there is a connection – negative or positive – between the mentioned factors?

8.Do you think the management (IT higher level managers) affect the resiliency of the dc?

   a. If yes how?

9. Can we categorized the mentioned factor?

   a. If yes, in what manner categorize the factor?

10. Do you measure your data center resiliency (Bank of Abyssinia)?

   a. If yes, how do you measure it?

11. Have you adapted a trend early on, for data center became resilient?

   a. If yes, in what way resilient DC in Bank of Abyssinia?