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

Architectural Framework for High Available Disaster Recovery Site: Case of Ethiopia Commodity Exchange (ECX)

By: Fitsum Seifu Weldetensay

September, 2021

ADDIS ABABA, ETHIOPIA

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

Architectural Framework for High Available Disaster Recovery Site: Case of Ethiopia Commodity Exchange (ECX)

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

By: Fitsum Seifu Weldetensay

Advisor: Temtem Assefa (PhD)

September, 2021

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES SCHOOL OF INFORMATION SCIENCE

Architectural Framework for High Available Disaster Recovery Site: Case of Ethiopia Commodity Exchange (ECX)

By: Fitsum Seifu W/Tensay

Name and Signature of Members of the Examining Board

Temtim Assefa (PhD) Advisor	_____ Signature	_____ Date
Dereje Teferi (PhD) Examiner	_____ Signature	_____ Date
Workshet Lamenew (PhD) Examiner	_____ Signature	_____ Date

Declaration

I certify that, to the best of my knowledge this thesis entitled –**Designing an Architectural Framework for High Available Disaster Recovery Site: Case of Ethiopia Commodity Exchange (ECX).** It has not been previously submitted in this University or other University for award of any Degree. It is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor, Dr. Temtim Assefa. The content of the thesis is the result of work which has been carried out since the date of approval of the research program. All the ethics procedures and guidelines have been followed properly while preparing this thesis.

Signature: _____

Fitsum Seifu W/Tensay

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

Advisor's Signature: _____ _____

Temtim Assefa (Ph.D.)

Acknowledgements

This thesis becomes a reality with the kind support and help of many individuals, I would like to extend my sincere to all of them.

Foremost, I want to offer this endeavor to our GOD Almighty for the wisdom he gave upon me, strength, peace of my mind and good health in order to finish this research. I would like to express my gratitude towards my family for understanding, care, prayers and continuing support which helped me in completion of this research and my beloved and supportive wife, who is always by my side when times I need her most and helped me a lot in making this study. I would like to express my gratitude towards my Advisor Dr.Temtim Assefa without his assistance, encouragement, dedicated involvement, understanding and guidance this work would have never been accomplished. My special thanks also goes to participants of this study at ECX their friendly and professional details for the subject matter. I am also grateful to my Instructors and classmates.

Fitsum Seifu

September, 2021
Addis Ababa, Ethiopia

Abstract

A disaster is anything that prevent an organization core business functions from operating properly, and disaster recovery planning are the most critical elements of a business but are often ignored. Therefore, businesses must make a well- structured plan and document for disaster recovery strategies and business continuation, even before a catastrophe occurs.

Much of the research undertaken previously are in financial sector disaster recovery planning, mostly they were focused on investigation for the implementation of disaster recovery planning in banking sector. This paper attempts to demonstrate ways of designing an architectural framework for the implementation of high available disaster recovery site with active-standby implementation architecture and business recovery strategies with minimum downtime and no data loss.

The study employed a design science research with case study method and purposive sampling was used to select participants from permanent employees of ECX in Addis Ababa head office and regional offices. Interview questions were designed using disaster recovery planning process to collect data, and the results were transcribed and converted into visualization.

Based on the findings, this study identified all business critical applications, the dependency of each critical business applications, resource mapping of each critical business applications and developed a framework of recovery strategies and finally tested the framework in a virtual environment.

Key word: Recovery Site, Disaster Recovery, Active-Standby, high available, recovery strategy.

Table of Content

List of Tables

List of Figures

List of Acronyms

AC	Air Conditioning
AD	Active Directory
App	Application
BC	Business Continuity
BCE	Basic Consolidation Estimation
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BRP	Business Resumption Plan
CBT	Change Block Tracking
CD	Central Depository
CNS	Clearing And Settlement
COOP	Continuity of Operations Plan
CP	Contingency Planning
CRM	Customer Relationship Management
DAG	Database Availability Group
DB	Database
DNS	Domain Name System
DR	Disaster Recovery
DRDAG	Disaster Recovery Database Availability Group
DRP	Disaster Recovery Plan
HA	High Availability
HADR	High Available Disaster Recovery
IBM	International Business Machine
ICT	Information Communication Technology
IIS	Internet Information Service
IP	Internet Protocol
IRP	Incident Response Plan
IT	Information Technology
ITDRP	Information Technology Disaster Recovery Plan
MTD	Maximum Tolerable Downtime
MTO	Maximum Tolerable Outage
NIC	Network Interface Card
NLB	Network Load Balancing
OEP	Occupant Emergency Plan
OS	Operating System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
UI	User Interface
VM	Virtual Machine
WRT	Work Recovery Time

Chapter One

1. Introduction

1.1 Background of the study

Business organization requires different resources like staff, infrastructure, and technology. Most organizations concentrate only on the technological front and expect technology to be the core aspect for success [4]. Some companies cannot tolerate any downtime, these include financial institutions, credit card processing companies and perhaps some high volume online retailers. They may decide that the cost for fully redundant systems is a worthwhile investment because the cost of down time for even five or ten minutes could cost millions of dollars [3]. Therefore, organizations have to be ready for any disturbances in technology that can happen due to unexpected events; the attacks of 9/11 are the best example. A strong and well-structured business continuity and disaster recovery plan would help an organization tackle those unexpected events [4].

In a study of companies that experienced a major data loss without having a solid DR plan in place, 43% never reopened, 51% closed within two years, and only 6% survived long-term [3]. These indicate that, in today's environment, no company can afford to ignore the need for DR planning, regardless of the company size, revenues, or number of staff [3].

The process of restoring an organization that has been harmed by a disaster to its pre-accident state is known as disaster recovery. Disaster recovery is a subset of business continuity that deals with the immediate consequences of an incident, such as recovering from a server outage, a security breach, or a storm.

Furthermore, throughout the planning stages of disaster recovery, there are normally multiple distinct processes, however those steps blur fast during implementation because the circumstances during a crisis is virtually never exactly as planned. As a result, disaster recovery entails halting the disaster's impacts as soon as feasible and dealing with the immediate consequences.

Disaster recovery is the process of bringing the organization that was affected by the damage to before-the-accident condition. Disaster recovery is part of business continuity, and deals with the immediate impact of an event like recovering from a server outage, security breach, or hurricane all fall into this category. Moreover, disaster recovery usually has several discreet steps in the planning stages, though those steps blur quickly during implementation because the situation during a crisis is almost never exactly to plan. Therefore, disaster recovery involves stopping the

effects of the disaster as quickly as possible and addressing the immediate outcome [3].

Many scholars said that, business continuity planning (BCP) is a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events [3]. Also which is defined as a prevention and rehabilitation plan against enterprise's internal and external threats, which secures business integrity and competitiveness. However, business continuity is mostly a preventive method, while disaster recovery is a restrictive one [5].

Business continuity planning (BCP) is an approach for developing and validating a strategy for ensuring continuous business operations before, during, and after disaster events. According to many academics, which is described as a strategy for preventing and resolving internal and external challenges to an organization's integrity and competitiveness. Business continuity, on the other hand, is primarily a preventative strategy, whereas disaster recovery is a restricting one [5].

Availability is the degree to which an application or service is available when, and with the functionality, users expect. Availability is measured by the perception of an application's end user [1]. Business continuity includes disaster recovery (DR) and high availability (HA), and can be defined as the ability to withstand all outages (planned, unplanned, and disasters) and to provide continuous processing for all important applications [2]. It is important to consider causes of both unplanned and planned downtime. Unplanned downtime includes hardware failures and data failures. Data failures can be caused by storage failure, human error, corruption, and site failure. Planned downtime includes system changes and data changes [1].

This paper explores the possible causes of system outage which is caused by disaster, planed, or unplanned activity and how to deploy possible recovery methods and techniques, which can be used to recover from disasters. Moreover, it involves identifying business critical applications and then designing architecture for implementation of a high available disaster recover solution with Active /Standby architecture. This study organized into the following chapters, first section is structured into background section describes the objectives, statement of problem, significance of study, and scope of study, chapter two illustrates literature review related to disaster recovery, disaster recovery planning, disaster recovery techniques, high availability, etc. In chapter three the type of selected research design and methodology is explained, chapter four deals about data interpretation, analysis, and experimentation of the results. Lastly Chapter five presents summary of the study, conclusion, limitation of the study, recommendations of the study, and future works of

the study.

1.2 Statement of Problem

Today most organizations depend on systems and online transaction processing, and any disturbance caused to it will halt the major operations and operating areas of that business. Hence, organizations have to be ready for any disturbances in technology that can happen due to unexpected events. A disaster recovery plan or any contingency plan would definitely help in preventing losses.

A disaster can occur at any time, and a business must be prepared for it [4], every business is unique and interaction issues between different software components can cause problems. At some point in time, mechanical devices will fail, electrical components are subject to environment changes such as heat, humidity, and electrostatic discharge that can cause premature failure. Cable damage can occur and connections may loosen. Environmental Issues Power Failures, network failures and air conditioning can cause a single system to become unavailable. Redundant measures can be taken to help address some of these issues [2].

The Ethiopian Commodity Exchange (ECX) is a platform where buyers and sellers can meet to trade, with quality, quantity, delivery, and payment guaranteed. ECX has 23 electronic warehousing centers and 7 electronic trading centers in Addis Ababa, Hawassa, Humera, Nekemt, Jima, Gondor, and Adama, as well as external connections with Ecx Authority, Coffee & Tea Development Authority, Woreda Agricultural Offices, and 16 government and private banks.

The company operates in different geographic locations and generates millions of dollars in annual export for the country. By designing a business continuity and disaster recovery plan that will address the major risks to the company in different locations, one can provide a path to recovery of the basic, mission- critical systems including business critical trading applications, industry standard applications, operating systems and overall IT infrastructures.

Until now there is no disaster recovery plan in place in any of the locations, as a result putting the organization in danger. Considering access to critical business applications to regional locations or branches, everything is accessed through the primary site. Due to current IT infrastructure, any service outage from the primary site will result in downtime. Moreover, because of the interconnection between different warehouses, trading centers, and other stakeholders, system downtime is not tolerated because it has a direct influence on Ethiopia's economy.

There has been some researches done in related areas by scholars. The Research by [6] mainly focus on an investigation of current status of Disaster Recovery Plan in Ethiopia Banking sector. The study found that 42.1% of the banks in Ethiopia implemented ITDRP however, 57.9% of the banks are still doesn't put in place, they are under progress. Moreover, the study identified that, even the 42.1% of banks who have ITDRP in place are still their plan is not practical, as it needs major technical improvements to meet its intended purpose. According to the study, concludes that, ITDRP is not enough emphasis given from top management; as a result ITDRP is not exercised well in banking sectors in Ethiopia.

A study by [7], the results show that 75.23% of the respondents analyzed both risks that threaten their business and the impacts they would pose on the business. Conversely only 51.04% of the participants agreed that, they have risk control mechanism in place. Moreover, 60.4 % of the participants have IT disaster recovery plan. Considering backup site, majority of the responses (38.1%) indicate the use of cold site, (14.3%) hot site and (12%) warm site. The top three system protection and resilience solutions the banks use are RAID system 73.58%, cooling, power & connectivity redundancy 66.04%, and virtualization 60.38%.

From the study, none of the banks have considered international standards during IT disaster recovery developments. In regard to the observed gaps and weaknesses, it requires management attention to regularly oversee implementation, update and testing of IT disaster recovery planning and preparedness in response to emerging threats.

The other study which focus on Information Technology Disaster Recovery Plan Framework for Banks [8], identified that, IT services and solutions in the banking sector should be protected to keep the business continuity in a disastrous scenario. As per the study, the findings indicated that Banks do not have IT DRP in place. Lack of framework, lack of focused group, lack of experiences, and lack of standardization are some of the challenges identified. Accordingly, the IT DRP framework is proposed for Banks of Ethiopia. The framework is confirmed and validated by the subject experts. According to the study, assessment of current practice was made and challenges were identified from one government-owned and other private owned banks in Ethiopia, and the study is not enough to reflect what's going in other Banks.

Different organizations developed and implemented disaster recovery plan and organization in our country can adapt that solution and implement it.

This research mainly focuses on designing an architectural framework for implementation of high available disaster recovery site with active-standby architecture. In this regard, this study will

explore and find answers to the following research questions:-

1. What are the key business processes and dependencies that exist between each process and which business processes require high availability during operation?
2. How would the business function in a recovery site? What would be needed in terms of staff, equipment, supplies, communications, processes, and procedures?

1.3 Objective of the study

1.3.1 General Objective

The general objective of this study is designing an architectural framework for implementation of High Available Disaster Recovery Site with Active-standby implementation architecture.

1.3.2 Specific Objectives

To achieve the general objective, the following specific objectives are designed to be achieved in this research:

1. Reviewing different Literatures related to implementation of high available disaster recovery site to gain in-depth understanding.
2. Identification of business critical application & their risks and analyzing dependencies that exist between each application.
3. Based on identified business critical application, developing recovery strategies.
4. Assess and recommend best practice of the implementation of high available Disaster recovery site.
5. Design the architecture or topology of existing system and developing the architecture of proposed high available disaster recovery site with Active-standby implementation method.
6. Implement the prototype of high available disaster recovery site with active-standby recovery using virtual environment.
7. Testing the feasibility of high available disaster recovery in virtual environment.

1.4 Significance of the study

In light of the significant gaps in academics and practice concerning the topic under consideration in Ethiopian context, this particular study would have notable significances. The study provides an insight of designing a High Available Disaster Recovery Site with Active-

standby implementation architecture and also helps in understanding possible recovery strategy of critical business operation when a disaster happen or application service outage occurs.

The significance and applicability of this research (designing a high available disaster recovery site) is very high for an organization having online transaction processing like ECX. For such organizations downtime is not tolerable because system unavailability for minutes will cost the organization millions of dollars and such a condition will have a massive impact on individual, organizational and national economy growth.

Moreover, by identifying what is needed in terms of staff, equipment, supplies, communications, processes, and procedures with key disaster recovery mitigation strategies, it would help how the business function in a disaster recovery site. The finding will also help the respective managements revise IT components of the business continuity strategies and follow-up their implementations according to the standardized modes of disaster recovery practices. This study could also invite interested researchers to explore more in related and similar areas.

1.5 Scope of the study

The study mainly focus on designing an architectural framework for implementation of High Available Disaster Recovery Site with Active-standby implementation architecture for ECX by identifying key business processes and testing the performance of the prototype in a virtual environment.

The study will not be involved in preparation of disaster recovery plan or recovery strategy document, it's only focused on designing high available architectural design and test in virtual environment. But, recommend best practice in implementation of disaster recovery planning and disaster recovery strategies and how an organization can benefit from that.

Since every business environment have its own key business processes, and this study is mainly focused on ECX and will not be applicable to other financial business sectors like Banks.

1.6 Organization of the study

This study is organized into five chapters. Chapter one is the introduction part of the document, it comprises background of the study, statement of the problem, Research questions, objectives of the study, Significance of the study, and Scope of the study. Chapter two deals about the literature review which mainly constitutes the theoretical and empirical reviews, conceptual

framework model of the study and related literature review subject to the study. Chapter three describes the research design & methodology applied to conduct the study. It also tries to address the research design strategy, approach employed, sample selection, data source and sample collection instrument, data analysis procedure, validity & reliability, and ethical consideration. Chapter four deals about data interpretation, analysis, experimentation of the results. Lastly Chapter five presents summary of the study, conclusion, limitation of the study, recommendations of the study, and future works of the study.

Chapter Two

2. Literature Review

2.1 Introduction

This section includes a review of the professional and academic literature related to the problem statement and purpose of this study. As technology continues to become more integral to corporate business operations at every level of the organization, the job of IT has expanded everywhere to become almost all-encompassing. These days, it's difficult to find an organization that technology does not touch. As a result, the need to plan for potential disruptions or system unavailability to a technology services has increased exponentially.

2.2 Disaster recovery, High availability, Business continuity

2.2.1 Disaster Recovery

According to [14] a disaster is anything that prohibits an organization's IT system from accessing vital business processes and activities. And disaster recovery is a collection of activities that take place before, during, and after a disruption event within an organization in order to get the business fully up and running.

In the event of a disaster, disaster recovery helps to address and use a set of resources, strategies, services, and procedures to recover and resume mission critical business applications at a remote site [2]. The action that must be undertaken to prevent the impact of the disaster and to initiate and apply recovery activities is included in the disaster recovery phase. Disaster recovery, moreover, include assessing appropriate alternatives and solutions to the significant disruption event, through damage assessment, risk assessment, and recovery activities.

The disaster recovery phase consists of three phases [4]: activation, execution, and reconstitution during a business disruption.

One of the activities undertaken during the activation phase of disaster recovery is disaster notification, which can be done by phone, email, or cell phone. Damage assessment is another activity that will be carried out during this phase; the assessment could be hardware or software, and during this step, components or elements will be replaced.

The execution phase of a disaster recovery strategy is when disaster recovery plans and procedures are carried out until regular operations are resumed.

The reconstitution phase of disaster recovery focuses on stopping or shutting down recovery plans or procedures, as well as returning business applications from the disaster recovery site to the production site.

2.2.2 High availability

Typically, the issue of developing a HA solution involves assessing and addressing all potential sources of downtime, as well as the system outage, which can be planned, unplanned, or disastrous [2].

Traditionally the terms high availability and disaster recovery are often used interchangeably, however, they are two distinct concepts practically: The ability of an IT system to tolerate all planned and unplanned failures is referred to as high availability, and it helps in the continuous processing of business-critical applications inside an organization [3]. Whereas After a catastrophic business interruption, disaster recovery involves using a set of policies, tools, and procedures to restore a system, a business application, or an entire datacenter to full function. However, continuous availability is a subset of business continuity [3].

2.2.3 Business Continuity

Business continuity is the capability of a business to endure outages and to operate important services normally and without interruption, in accordance with predefined service-level agreements [3]. Business continuity is a way for establishing and validating a business's ability to operate continuously before, during, and after a potentially catastrophic incident. It specifies an organization's ability to withstand all outages and redirect important business applications to an alternate site until the business return into normal operation and the operational factors will enable a business to function normally in order to produce income [31].

High availability, continuous operations, and disaster recovery are depicted in Figure 2.1. To achieve the desired level of business continuity, a collection of services, software, hardware, and procedures must be selected and executed, and they must be established and exercised on a regular basis in line with a document plan [2].

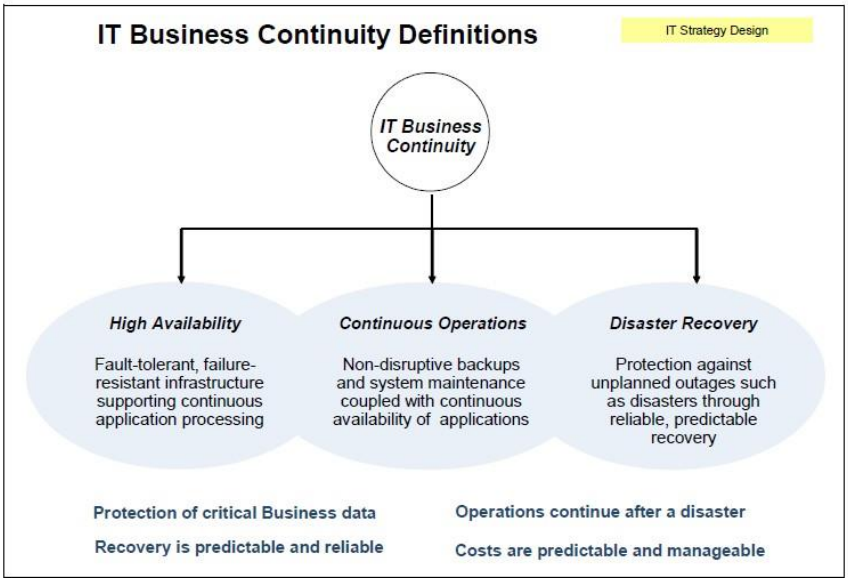

Figure 2.1 Inter-relationship of High Availability, Continuous Operations, and Disaster Recovery

2.2.4 Business continuity planning and Disaster recovery planning

The ability of an organization to continue operating regardless of the type of a potential business disruption is the focus of business continuity. Business continuity planning is also a codified approach that may be studied and practitioners certified as a result. Because it deals with mitigating the impacts of a disaster or incident, disaster recovery planning is sometimes considered a subset of business continuity planning. It is generally acknowledged that business continuity measures and should commence once the impacts of the disaster or event have been addressed [16].

Business continuity management covers the overall process of managing a disruption and re-establishing critical business functions. A key part of any organization response to a disruption is providing the necessary resources for the organization to continue delivering critical business functions. Disaster recovery is one element of business continuity management, it is the mechanism that organizations use to recover their systems following a major disruption [34].

2.2.5 Disaster recovery plan

Planning for IT disaster recovery is a challenging task. And an organization's ability to respond quickly and effectively to a disruption is enhanced by having a disaster recovery strategy. The need of disaster recovery planning for the recovery of these systems grows as businesses become more dependent on IT systems to operate their operations [34].

Disaster Recovery Plan is a plan designed to recover all the critical business processes or business critical applications during a disaster within a short amount of time. Disaster recovery plan has all the procedures required to handle the emergency situations. Mostly the DRP has technology oriented methodologies and mainly concentrates on getting the systems up as soon as possible, within a reasonable amount of time (RTO and RPO). RTO and RPO are the recovery time objective and recovery point objective, which are the targets of DRP [4].
Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, and facility at an alternate site after an event of disruption [25].

2.2.6 Business continuity plan

The activities required to keep the organization going during a period of displacement or disruption of normal operations are referred to as business continuity. And BCP helps in the continuation of operations of a business after a catastrophe event or disaster [4].

The process of building a practical plan for how the firm may prepare for and continue to operate after an interruption is the main emphasis of business continuity. During a crisis, an organization must remain operational; if it does so for even a day or a week, there is a good possibility it will lose profits and be forced to shut down. As a result, an effective BCP strategy can be used to effectively execute and maintain business activities [4][34].
The Business Continuity Plan (BCP) is more significant because it focuses on keeping an organization's business functions running during and after an interruption. A business continuity plan (BCP) can be created for a single business process or for all important business processes. As a result, IT systems are taken into account in the BCP in terms of their ability to support business processes [25].
A business continuity plan (BCP) is a set of activities that develops, tests, and maintains strategies that allow a company to continue operating in the event of a disaster and also to [18]:

- Respond to a major disruption with the least amount of loss of life and damage to resources.
- Recover, resume, and restore functions on a timetable that ensures the organization's long-term survivability.
- All stakeholders should be informed about the crisis.

Differences between DRP and BCP

Disaster Recovery Plan	Business Continuity Plan
Activities are pre-planned to react to disasters.	Planning on mitigating risk for the assets, business processes that will adversely impact company, if a disaster happens.
DR plan starts with IT, not because other aspects are not important, but because IT is easiest to recover, and impact is also more.	BC plan is not an IT process; it includes the complete business as a unit.
A DR plan can be built upon a strong business continuity plan.	The business continuity process has a series of DRPs.
Disaster recovery is data centric.	Business continuity is business centric.
Main idea: Recover from disasters.	Main idea: Continue critical business operations.

Table 2.1 Difference between Disaster recovery plan and Business continuity plan [4]

2.3 Business Requirement Gathering using DR Planning Processes

2.3.1 Risk Assessment

Risk management is a business process in which an organization addresses all of the risks and hazards that it faces today. The four phases of a basic risk management approach are threat assessment, vulnerability assessment, impact assessment, and risk mitigation strategy formulation. To identify threats for a business continuity and disaster recovery strategy, we might use the framework of people, process, technology, and infrastructure [3].

It is a key fundamental component of an organization BCP program, and risk analysis is the starting point in disaster recovery planning phase, which involves detail analysis of risks, vulnerabilities (exposures), and is a component of risk assessment. Scholars suggest that, natural and environmental threats to the business must be assessed not only in terms of how they directly impact the company, but also how they indirectly impact the company[3] [36].

Based on study from [3], indicate that disasters or business disruptions to consumers, partners, and vendors can have a significant influence on a company's bottom line and should be evaluated. According to the information provided in [3] four major types of tools can be used to assess threats: questionnaires, interviews, document reviews, and research. Each will yield specific data. A comprehensive review will use all four methods and combine data.

2.3.2 Criticality Categories

In business continuity plan analyzing the critical functions is first, essential functions will be second. It's important to have an idea of rating system before review of the business functions so that the organization can spend the appropriate amount of time and energy on mission-critical functions and less time on minor functions. Bellow the categories are clearly defined and that there is a shared understanding of the proper use and scope of each. According to [3], here is one commonly used rating system for assessing criticality:

- **Category 1:** Mission-Critical: Mission-critical business processes and functions are those that have the greatest impact on company's operations and potential for recovery, recovery time of 0–12 hours.
- **Category 2:** Essential Functions–Vital: Some business functions may fall somewhere between mission-critical and important, recovery time of 13–24 hours.
- **Category 3:** Functions–Important: Important business functions and processes won't stop the business from operating in the near-term but they usually have a longer-term impact if they're missing, recovery time of 1–3 days.
- **Category 4:** Desirable Functions–Minor: Minor business processes are often those that have been developed over time to deal with small, recurring issues or functions recovery time of, more than 3 days.

2.3.3 Business Impact Analysis

The Business Impact Analysis (BIA) method entails establishing an organization's Critical Business Functions and evaluating those operations in light of risk assessment information. Critical objectives, deadlines, dependencies, and impact must all be understood and studied for each essential business operation. Furthermore, the potential for business disruption will be assessed [3][36].

The business impact must be assessed after identifying risks and threats to critical business processes. The impact of important business functions being disrupted is examined and prioritized in order to design risk mitigation solutions [3]. More importantly, according to [35] its a management-level analysis of organizational business processes that assesses the risks of important business functions being disrupted, taking into account the effects of capability loss

over time, as well as resource requirements and interdependencies.

There is an optimal point between the cost of downtime and the cost of recovery. The longer systems are down, the more expensive it is for the company. The shorter the required recovery time, the more expensive it is for the company. Therefore, the intersection of the cost of downtime and the cost of recovery is the optimal point. This is not always easy to determine but the concept helps in the planning efforts [3].

According to [3][35] a system recovery of critical business processes use parameters such as:

Recovery Point Objective (RPO) - The maximum data loss that can be tolerated is based on backup data requirements. And also, it could be defied as, after such a disruption, the point at which an organization must recover data.

Recovery Time Objective (RTO) - The amount of time it takes to recover critical systems. Alternatively, how quickly must each technology service be available?

Work Recovery Time (WRT) - The time it takes to recover lost data (based on RPO) and enter data as a result of work backlogs (manual data generated during system outages that must be entered).

Maximum Tolerable Downtime (MTD) - The duration of the RTO plus the WRT.

2.3.4 Backup and Recovery Considerations

There are numerous areas of the company that may require alternate business processes to be developed and/or available. These areas are sometimes overlooked in planning. Customer service, administration, essential equipment, and premises are four areas that require specific attention in the risk mitigation planning. IT recovery systems are numerous and include (among many others) alternate sites, disk system solutions, clustering, virtualization, and vaulting [3].

2.3.4.1 IT Recovery Systems

Undoubtedly there are many IT recovery systems, but as part of risk mitigation strategy development, we should scan the technological horizon to see what's available in today's market. Sometimes IT departments develop risk management strategies based on current technology and never update those strategies. Systems put in place five years ago that are not reviewed and updated can inject additional risk into the organization, and puts BC/DR plan at

risk [3].

2.3.4.2 Alternate Sites

The decision of whether or not to build alternate sites and whether or not to have a dedicated site that is wholly owned by the company is one of the most important decisions that an organization must make. And Alternative disaster recovery sites are available in a wide range of sizes and designs. Operations at the disaster recovery site can differ from one organization to another, depending on the demands and finances [33]. Selection criteria are the elements designed to determine how to choose the best alternate site solution for the company. During site selection, cost, technical and functional requirements, timelines, quality, availability, location, and other aspects are all taken into account. Other factors to consider in this regard include connectivity and communications requirements, as well as recovery requirements such as the maximum acceptable downtime [3]. There are different site redundancy with data replication strategies, and summarized as follows in table 2.2.

2.3.4.2.1 Fully Mirrored Site

Mirrored sites are completely redundant sites that replicate the live site's activity. By far the most costly and comprehensive IT risk mitigation technique. This method may be appropriate for some businesses. Because every transaction that occurs on the live site is likewise completed on the mirrored site simultaneously, mirrored sites give the highest level of availability (and thus risk mitigation) [3].

2.3.4.2.2 Hot Site

A hot site is typically a site leased to the company for emergency needs by a commercial vendor. The vendor will ensure that the technical configuration and connectivity are identical, allowing IT functions to be moved to the commercial location within a specific time limit, usually one to four hours. [3]. A hot backup site typically provides a set of mirrored stand-by servers that are always available to run the application once a disaster occurs, providing minimal RTO and RPO, according to [33], RTO would be within 12 hours and the acceptable maximum RPO would be 10 minutes. Hot standbys typically use synchronous replication to prevent any data loss due to a disaster [32].

The data is delivered to both the primary and backup servers at the same time. As a result, data is

always identical in both servers. In the event of important data, this redundancy approach is employed [10]. These locations usually have ample room for hardware, infrastructure (racks, cables, phones, printers), and support workers [3].

2.3.4.2.3 Warm Site

Warm sites are facilities that are only partially equipped, with some or all of the essential equipment located at the primary site. Warm sites are commonly employed for less important services during normal operations and then taken over for key IT functions after a business disruption. In the case of a business interruption or disaster at the primary site, the secondary site may quickly fire up the server, restore from the most recent backup, and continue important operations [3]. For this option two servers are used: the primary and the secondary. The former contains the original data. The secondary captures data from the primary server at regular intervals of time, without causing its interruption [10].

Depending on the required RPO, a warm backup site may use synchronous or asynchronous replication strategies to maintain state current. Standby servers are ready to execute the program in the event of a failure, but they are merely stored in a "warm" condition and may take minutes to bring up [32]. And according to [33] RTO should be within 24 hours and RPO should be 5-30 minutes.

2.3.4.2.4 Cold Site

In the event of a disruption, a cold site is launched. These sites are the cheapest to set up before an emergency, but they take the longest to restore after a disruption [3].

As in warm standby, the primary server's data is replicated to the secondary server on a regular basis.

Mirroring, on the other hand, is used less commonly than warm standby [10]. If you only need to recover for three or four days, this may be the most cost-effective option. However, the BC/DR strategy should include provisions for how and where a cold site may be established, and this option should be chosen [3]. In a cold backup site, data is sometimes only copied on a periodic basis, resulting in an RPO of hours or days. According to [33] RTO is 2 hours to 3 days and RPO should be within 24 hours. Furthermore, servers to run the application after a failure are not quickly available, and hardware may be retrieved from storage or repurposed from test and development

systems, leading in a long RTO [32].

Site	Cost	Hardware Equipment	Telecom-munications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

Table2.2: Alternate Site Selection

2.4 Data center topology options for High Available Disaster Recovery

When a disaster occurs in any business environment, the topology and configuration choices we made will determine how our application recovers. To choose the best one for our needs, we must first understand the costs and benefits of each configuration. A disaster recovery topology with two data centers configuration of active-active or active-standby are two possible configurations as presented in Figure 2.2.

In both cases, data is continuously replicated between the two data centers. In the event of an outage or application failure, pre-application work is completed to ensure that the standby data center is prepared to serve the request. The standby data center can operate in either a hot or cold standby mode [9].

The order application and associated services are deployed to both data centers in the hot standby option, but the load balancer only directs traffic to the application in the active data center.

The advantage of this configuration is that the hot standby data center is ready to be activated in the event of a disaster in the active data center. The DR procedure only requires reconfiguring the load balancer to redirect the traffic to the newly activated data center. The software license is applicable to both data centers, although only one is actively in use [9].

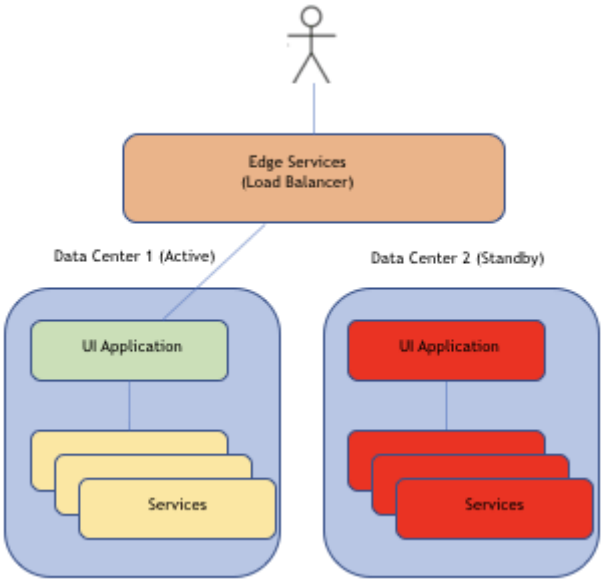

Fig 2.2 Active-standby topology configuration of two Datacenter

The order application and associated services are deployed to both data centers in the cold standby option, but are not started in the standby data center. If the active data center suffers a disaster, the DR procedure entails restarting the application and services as well as reconfiguring the load balancer to redirect traffic. This option is less expensive in terms of software licensing and data center operations costs, including personnel. However, depending on how quickly the cold standby data center and the order application can be started and activated to process requests, application availability may suffer.

2.5 Architecture of SAN to SAN Replication

As shown in Figure2.3, presents architecture of high performance servers connected to SAN storage system, where the storage system automatically replicates data from Production site to DR site. However, this configuration only ensure that data availability but not server availability. Manual intervention step would be required to stop the replication, enable storage access from DR sites and manually powering up each of the VMs. This architecture is Active-Passive replication in between SAN storage system. This architecture achieves not only business continuity of disaster recovery (BCDR) but creates an Active- Standby environment by replicating data that is change by block level from the production site to the DR site [28].

Since replication of data happen in certain interval in between SAN storage system, it confirms that there is a data consistency in primary site and DR site. More importantly with minimum

human intervention allow to run the business from DR site, whenever system outage occurs in production site.

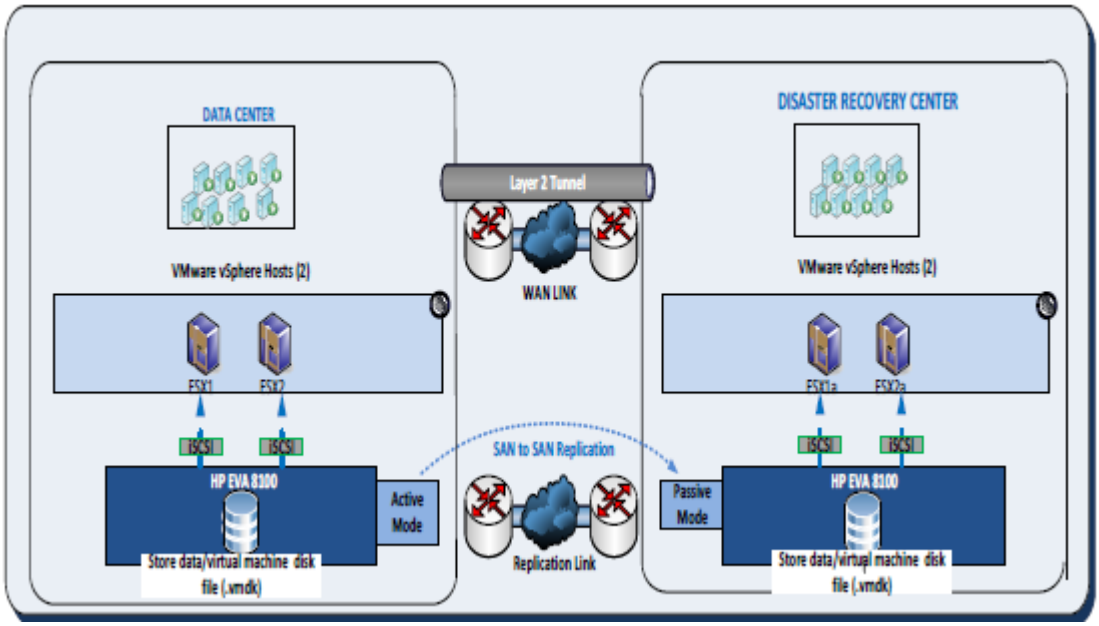

Figure 2.3 Architecture of SAN to SAN Replication

2.6 Related literature Review

There are few pieces of local researches have been done in related to Disaster recovery, the first one is Disaster recovery planning (DRP) investigation and assessment [6], the objective of the study was investigating the current ITDRP status in Ethiopian banking sector located in Addis Ababa City, the study methodologically used a mixed research design. The researcher took a total of nineteen respondents from nineteen banks in Ethiopia, the questioners which contained both close-ended and open-ended questions. Technically, the respondents were selected through purposive sampling. For data analysis of the quantitative data findings were analyzed through SPSS software program, version 20; whereas, the qualitative findings were using a simple thematic analysis approach. After the careful assessment of findings, the study found that 42.1% of the banks in Ethiopia implemented ITDRP however, 57.9% of the banks are still doesn't put in place, they are under progress. Moreover, the study identified that, even the 42.1% of banks who have ITDRP in place are still their plan is not practical, as it needs major technical improvements to meet its intended purpose. According to his study, he concludes that, ITDRP does not get

enough emphasis given from top management; as a result ITDRP is not exercised well in banking sectors in Ethiopia.

As a weakness it observed that, the research mainly focus on investigation of the current ITDRP status in Ethiopian banking sectors specially those located in Addis Ababa, it doesn't consider those located outside Addis like in big regional cities of Mekele, Hawasa, Adama, Diredawa, etc. Moreover, the study mainly focused on banking sectors only but there are microfinances, insurances, import export companies, Commodity Exchange organizations, etc.

A study by [7], the purpose of the study is to assess IT disaster recovery practices of Ethiopian commercial banks. The study employed qualitative method to investigate the IT disaster recovery practices and preparedness in 18 Ethiopian commercial banks. A total of 72 participants of which 54 respondents with relevant expertise in the field and 18 IT managers were selected. For the study the researcher used purposive (non-probability) sampling. Data was collected through questionnaires and semi-structured interviews, and it was analyzed using IBM SPSS Version 23 and Microsoft Office Excel 2007. The results of the analysis were displayed using frequency tables, pie charts and bar graphs. The results of the study show that 75.23% of the respondents analyzed both risks that threaten their business and the impacts they would pose on the business. However only half (51.04%) of the respondents agreed that they have risk limitation mechanism in place. 60.4 % of the respondents have IT disaster recovery plan however the human aspect of IT disaster recovery planning, plan testing and updating are identified to be components overlooked by the banks.

Considering backup site, majority of the responses (38.1%) indicate the use of cold site, (14.3%) hot site and (12%) warm site. The top three system protection and resilience solutions the banks use RAID system 73.58%, cooling, power and connectivity redundancy 66.04%, and virtualization 60.38%. None of the banks have considered international standards during IT disaster recovery developments. From the study show that none of the banks have considered international standards during IT disaster recovery developments. In regard to the observed gaps and weaknesses, it requires management attention to regularly oversee implementation, update and testing of IT disaster recovery planning and preparedness in response to emerging threats.

A study by [30] Datacenter disaster recovery and major incident management, the main objective of the study was how to recover a datacenter from major disruptions and how to build a disaster

recovery of most of business critical systems by using predictive research method.

The organization had identified the importance of business continuity planning with two key deployment techniques were identified for the IT system, which were building a disaster recovery having faster recovery time & recovery site and incident management system.

The primary research method for this study was design science research method, the main focus of this study was building a datacenter to support business continuity system, and the design parameters were time and resource which are limiting factors.

The study uses case study with predictive research method which helps to estimate the possible requirement for the new datacenter. The basic environmental data was available for the current platform, but with the pre-existing complex environment, it's very difficult to predict how the end result will be. Predictive research is to take the data you have and to predict the data you don't have. The data collection of the study was from the main datacenter located in southern Finland, the Case study is focused on sites Vantaa and Lahti and disaster recovery environment is limited to only certain virtual machines, Data gathering from virtual was done by RVTools which includes information such as virtual machine name, cpu, memory & network configuration. Based on this data, estimation for disaster recovery capacity planning was made, which have been identified as most business critical. The overall platform consists of 39 VMWare hosts on 18 sites, hosting 621 virtual machines in total.

The researcher mentions that, based on the result obtained RPO and RTO heavily controlled by the budget defined and based on what will be accomplished with certain amount of budget for the DR site. The estimation was presented with multiple options for the business and top management decision for acceptable DR solution. As said by the researcher, there is a plan to expand the DR solution to other sites and do annual testing of the service under DR scope.

The researcher tries to answer to research questions and come to a conclusion as follows:

- Disaster recovery and incident management systems are edge solution to an organization, without having a proper disaster recovery and incident management system organization may lose lots of revenue. Therefore, organization should start to think to establish such system and requires a continuous follow up.
- The importance to building a disaster recovery datacenter is recovery of the business into normal operation, the implementation should be started first by building primary

site and implementing DR site located within the organization (on premises) or cloud solution (Microsoft Azure or other).

- Once the technical requirement of building a disaster recovery solution is identified, it may take from few weeks up to moths but building a new datacenter is a very challenging task because the space requirement is a big step to establish.
- When an organization ready to invest on implementation of DR solutions, IT professionals should start to think about technical requirement with future expansion and when there is correct technical solutions are in place it's easy to manage the upcoming IT solutions. Moreover, IT professionals should aware the business that, business continuity is more that technical solutions.
- The only way to ensure that business continuity is implementing properly, when the documentation is reviewed and updated accordingly.

2.7 Conceptual Framework

A framework define as, the structure of a particular system in which it can provide the true picture of set of components, functions or applications work together to form the system. A framework of a research is the structure of a research that guide the researcher to follow while selection of study questions were designed, method of variable measuring were selected and data analysis applied [10][11].

A theoretical framework tells the theoretical assumptions that the research is based and the necessary research method guide the researcher to test his assumptions and the way how his assumption connects to the existing knowledge [10]. It is a theory that the researcher choose to guide his research which derived from set of concepts or same theories [11].

A conceptual framework is a set of interrelated concepts that bring together to explain existing business problem, or to give an in depth description of existing research problem by guiding the researcher how it goes and for the readers guide what and how is done so far. And also it is an interlinked concepts together which can provide comprehensive meaning to a certain phenomenon. While building a conceptual framework, the researcher may depend on his own idea, or may adapt an existing model or method as conceptual framework if and only if the model is specific to what to study trying to accomplish [10][11].

The framework Figure 2.4 presents, set of interrelated steps to follow to identify business critical application, to describe the concepts and draw the relationship that occur between the platforms

and dependencies that exist among application. Moreover, this framework helps to conceptualize the way how interaction exists among the different business critical applications and the steps & the concepts are drawn. More importantly it helps to develop recovery strategies of each critical business applications. Each step of the process were further explained in the recovery strategy section of this document in page 43.

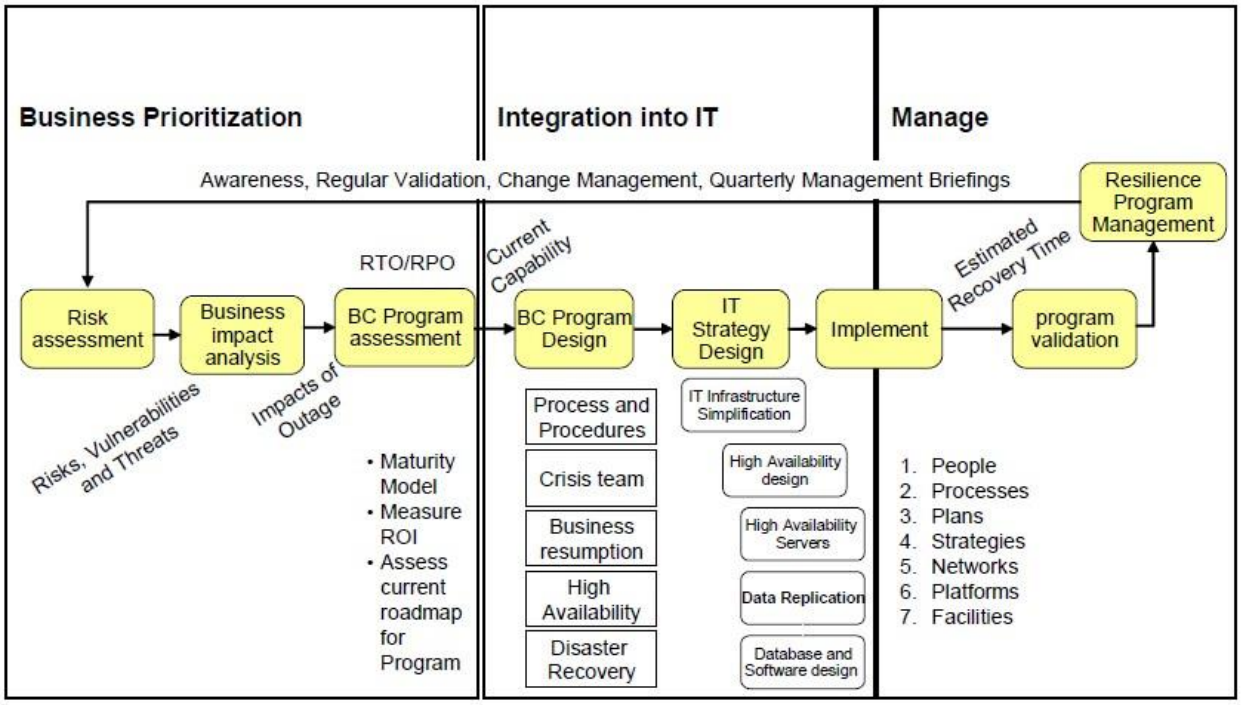

Figure 2.4 IBM Global Technology Services, Business Continuity and Recovery Services framework [29].

2.8 Chapter Summary

This chapter presents literatures reviews related to high availability & disaster recovery, and try to show key terms such as Disaster recovery, High availability, Business continuity and the different planning methods: Business continuity planning and Disaster recovery planning. Disaster recovery planning process to get understanding of risk assents, business impact assessment which helps to develop recovery strategies and conceptual framework of the study.

Chapter Three

3. Research Design and Methodology

3.1 Introduction

The purpose of this chapter is to design appropriate research methodologies to carry out the study in line with the research objectives and research questions. The methodology employed to answer the research questions is presented in this chapter. The chapter divides into major sections. The first section of the chapter is research approach followed by the research strategy of the study. The next part is about sample selection and sample selection procedure, after that, data collection, next section data analysis, and the last section is about reliability & validity of data and Ethical consideration.

3.2 Research Design

Selecting the appropriate research methodology in a research greatly depends on the nature of the research and the type of research method selected. For this study, Design science research selected, it involves in the creation of artifacts (methods, models) to solve organizational business problem. It is a two steps process, in which it built an artifact for specific purpose and evaluates the performance of the artifact to measure how well the artifact performs.

Moreover, design science research activities mainly focused on improving the performance of a system through building and evaluating the artifact. While designing artifacts, a model define set of prepositions or statements defining relationship in between constructs and a method defines set of steps to accomplish a task. During evaluation of artifacts the performance can be measured in terms of functionality, completes, consistency, accuracy, usability, etc and these parameters considered as evaluation metrics, and the metrics define what we are trying to achieve.

The process cycle for design science is divided into five steps, as shown in Figure 3.1: awareness of problem, suggestion, development, evaluation, and conclusion.

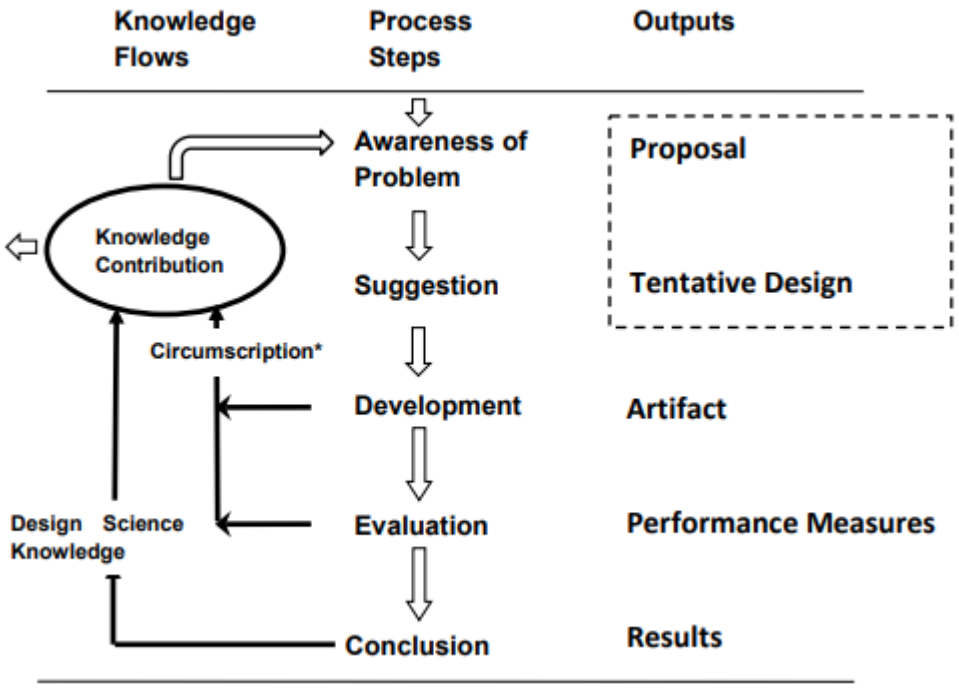

Figure 3.1 Design Science Research Process Model (DSR Cycle).

The first phase in process cycle for design science is awareness of problem, in this study came from the disaster recovery requirement of the organization. The aim of this study was how to build a high available disaster recovery solution.

Suggestion phase was introducing the suggested solutions to the organization for development of a high available disaster recovery of critical business applications. There are different suggestions were presented with best practice system implementation from different platform before the actual implementation of the model.

After critical business application has been identified and their recovery priorities or recovery strategies studied the actual development of the plan start. Building the actual high available disaster recovery solution to each business critical application was the main part of the development step.

Once all the necessary hardware and software requirement for all critical business application were identified and implemented, the next step will be evaluation of the performance of the newly implemented system. This stage mainly focused on evaluation of artifacts, to measure how well the new system will able to explore and solve existing organizational problems.

The final stage of design science cycle is conclusion phase, which mainly focus on result analysis

and final conclusion of what has been found at the end.

3.3 Research Strategy

Researchers use several types of study designs which include, design science research involves in the creation of artifacts to improve the performance of information systems problems and those designed artifacts are useful and fundamental in understanding that problem.

Among the different research strategies, case studies were used in design science research to generate a hypothesis at early stage of research process and to validate a method. A case study design helps to develop an in-depth description and analysis of a case research subject to explore what, how, or why research questions. Case studies are description of an individual case and its analysis in a comprehensive way. In a case study, single or multiple cases may be investigated. Single case refers to a singular case study and multiple case studies are used to describe several cases in the study.

A case study design strategy was suitable for this study because it helps to explore ways in which IT managers develop and implement disaster recovery plans, also helps to develop disaster recovery strategies of business critical applications. And the case study of this research mainly focused on primary site or primary datacenter of ECX.

3.4 Sample Selection

The first step, in sampling is to define the target population. The target population is the group of interest to the researcher, the group to which would like the results of the study to be generalizable.

Participants were chosen from their perspective division by the researcher to gain an in-depth understanding of existing core business processes and applications. The goal of this study is to create a high-availability disaster recovery site for critical business applications. As a result, participants for this study will be permanent employees of ECX with prior expertise working with critical business application and experience of disaster recovery of critical business applications.

Thus, for the purpose of this study as presented in Table 3.1 participants were selected from IT System Administration, Network Administration, Application Development, IT Security, IT Audit, Risk Management, BIS, Database Administration, and IT Support Team who meet criteria that will provide a sample that is likely to yield the type of information required to achieve the

purpose.

No.	Location	Department/Division of participant	Job position	No. of Participant
	Head office	IT Infrastructure & Support	Management Level	1 IT officer (Top)
				1 IT Manager
1	Head office	IT Infrastructure & Support	System Administrators	1 Senior Position
				3 Specialist Position
2	Head office	IT Infrastructure & Support	Database Administrators	1 Senior Position
				1 Specialist Position
3	Head office	Application Developers	Application Developers	1 Manager
				2 Senior Position
				4 Specialist Position
4	Head office	IT Infrastructure & Support	Network Administrators	1 Senior Position
				3 Specialist Position
5	Head office	IT Security	IT Security	1 Manager Position
				2 Specialist Position
6	Head office	Trading Operation & Data warehouse	Manager, Trading Operation	2 Manager Position
7	Branch office	Regional Trading Centers	Managers, Regional Trading Centers	4 Manager Position
8	Head office	IT Audit & Risk Management	Manager, Head Office	2 Manager Position
9	Head office	Business Development	BIS, Manager	1 Manager Position

Table 3. 1 Participants of the study, permanent employees of ECX.

3.5 Sampling Procedures

The sampling procedures purpose is to describe what method used to obtain the sample. However, knowledge of the major sampling procedures is a prerequisite to developing an appropriate description of the sample. One desirable characteristic of a sample is representativeness. Representativeness enables results from the sample to be generalized to the population.

3.6 Purposive Sampling

The target population for this study is permanent employees of ECX who are IT teams of application developers, Network admins, System admins, DB admins, Security admins, and Manager & above position of other departments working in Addis Ababa city. However, from district managerial positions, Branch Manager intentionally included to the study because the assumption that the effect of the leaders on organizational success in terms of DR implementation is significant. And the sampling method will be Purposive sampling which is nonprobability sampling method, and useful of selecting samples based judgmentally on their merits or special experiences that might have in relation to the research topic. Purposive sampling involves selecting a sample based on the researcher's experience or knowledge of the group to be sampled. Moreover, purposive sampling is also proved to be effective when limited numbers of people required during gathering primary data.

3.7 Data Collection Methods

While conducting a research, data collection is one of the most important aspects in conducting a research work. Data-gathering strategies enable a researcher to collect information in a systematic manner. Regardless of how data is defined, reliable data collection is critical to ensuring the integrity of research.

Data collection of this study was based on the use of semi- structured interviews that aimed to encourage participants to provide their own views and perspectives of their experiences working in an IT work environment. From a number of data collection methods, this study employ interviews, onsite observation, and Document analysis which includes content analysis of research papers which was previously done by different scholars that are undertaken for the purpose of data collection.

Interviews are very helpful for learning more about a participant's experiences. And the interview questions were developed based on the problem findings of previous studies that were discovered. And those findings are mapped to disaster recovery planning process steps as mentioned in appendix A of this document, which includes project initiation, risk analysis, business impact analysis, planning, Maintenance, Training, Testing, and Auditing. The researcher assumes that, following this process will allow identifying what should be done in each step of the process and

helps to develop recovery strategies.

Furthermore, before beginning the interview, the researcher explained the concept or the idea behind the research, as well as the purpose and length of the interview.

3.8 Data Analysis Approach

In research, data analysis involves preparing and organizing the data through transcription of interviews, and then representing the data in figures, tables, or a discussion. The type of data collected for this research study is qualitative data which refers to all non-numeric data or data that have not been quantified. And collect the data through observations, interviews, and document analysis which requires the data to be classified & analyzed through the use of conceptualization and summarize the findings primarily through narrative or verbal means.

All of the processes and tools used in this process enable the researcher to interact with the data in order to comprehend it, integrate related data drawn from various transcripts and notes, and identify key themes or patterns for further investigation. During data collection of the study, responses were categorized into specific themes to create clear understand of data interpretation to gain an in depth understanding of the study. Further, during the study data triangulations for analysis were used to identify existing system configuration information to validate what was obtained.

3.9 Validity and Reliability

Reliability and validity are ideas that are used to assess the quality of research. And an attempt to analyze the "accuracy" of the findings, as best stated by the researcher and the participants, in the study. Validity and reliability indicate how well an instrument measures something. Reliability is about the consistency of a measure, and validity is about the accuracy of a measure.

Reliability reflects the consistency of results and the result is not varying over time. Or the reliability of a research instrument focuses on, the extent to which the instrument gives the same results on repeated trials. The more errors found in a test, shows the more unreliable are the test. Validity refers to the trustworthy or accuracy of a test.

In addition validity explains how well the collected data covers the actual area of investigation.

Validity intended to define as “measure what is intended to be measured”. There are different types of validity and this study considers a content validity, which is defined as “the extent to which an instrument's components reflect the content universe to which the instrument will be generalized”. It is strongly advised in the field of information system to use content validity when developing a new instrument. Moreover, judgmental approach will be used to establish content validity. The judgmental approach begins with a review of the literature and is followed by an evaluation by expert judges.

As previously stated, while designing interview questions for this study, interview questions were designed based on previous study findings via literature review and followed by delivery of the document to staff with prior experience working with IT thesis research and disaster recovery of business critical applications. Furthermore, the interview questions were redesigned in response to feedback from experts in the field.

3.10 Ethical considerations

The study has attempted all the necessary precautions to protect the study participants from such sort of problematic encounters by applying certain measures. Moreover, they have been assured that no meaningful damage would be inflicted on them because of their participation in this particular study by boldly explaining to them the apparent purpose of the study (which is actually for academic purpose) and ensuring the confidentiality of their identity and whole part of the information they provided for the purpose of undertaking this study.

3.11 Chapter Summary

This chapter presents initially Research Design, followed by Research Approach, Research Strategy, Sample Selection, Sampling Procedures, Data Collection Methods, Data Analysis Approach, Validity and Reliability, and finally on Ethical considerations of the study.

Chapter Four

4. Data Presentation, Analysis, and Results

4.1 Introduction

This chapter presents the results of the study based on data collection using interviewing of core business units of the organization and document analysis. The chapter subdivided into major sections, initially focus on interview questions & response with further explanation, after that designing a conceptual framework of critical business applications, followed by proposing disaster recovery strategies, and then designing high level architectural framework for existing & proposed system, and finally presenting implementation & experimental setup of proposed system in virtual environment.

4.2 Data from Interview

From a number of data collection methods, this study used document analysis, onsite observation, and interview questions which contain open ended questions. And this section mainly focused on the analyzing of the open ended responses. Therefore, validation of findings by providing further explanations to the results from interview and recommendation from subject experts through further investigation of the results has been done at this stage.

4.2.1 Project Initiation

In project initiation, based on interview question of how the disaster recovery initiated, how do you identify who will be working at the original site and who will be working at the alternate site? What are the key skills, knowledge, or expertise needed to recover?

The IT Infrastructure Manager explained that, *they are currently forming a disaster recovery team, and if a system outage occurs, the team will be selected based on academic qualifications, industry hands on experience, and knowledge of business operations. As he stated, the abilities or knowledge required include System Administration, Network, Database, Application, and Storage Administration. The system and storage administrator should take the lead.*

In IT project management system, one of the basic steps is creating a project team and a project success or failure highly depends on the project team because it's mandatory to get input from various subject matter experts during the course of the project. For the project plan to be

successful, we must work with people from all key areas of the company. The specific types of teams required are based on the system affected. The size of each team, specific team titles, and hierarchy designs depend on the organization. In addition to a single authoritative role for overall decision-making responsibility, including plan activation, a capable strategy will require some or all of the functional groups.

4.2.2 Risk Assessment

There are variety of IT system disruptions, ranging from short-term to long-term system unavailability, many of this disruptions will be minimized or eliminated through technical, management, or operational solutions as part of risk management effort. It's virtually impossible to completely remove all risks but is possible to mitigate risks. Based on the Information from, Risk Management Team Manager, *They have policies and procedures in place to identify hazards in IT infrastructure, security, application development, and network systems.* As he stated, *after risk has been identified, mitigation techniques would be developed in consultation with IT divisions. In terms of disaster recovery, numerous hazards have been discovered so far, owing to the fact that the BCP is still being developed and is unable to solve those difficulties.* Without having a proper BCP plan in place, it's difficult to address issues related to any business disruptions which could be power outage, system crush, or data theft.

Security Manager added his view as, *unauthorized access, scalability issues with various platforms, a lack of defined BCP, misuse of business vital systems, whole or partial company interruption, data loss, hacking, theft, and other serious threats have all been documented. Furthermore, in a conversation with the Application Development Team Manager, mentioned that due to the dynamic nature of the trading model, the application system changed constantly, making it unable to meet user needs.*

To successfully determine the specific risks to an IT system during service interruption, a risk assessment of the IT system environment is required. During this process there is total process of identifying, controlling, and eliminating or minimizing uncertain that may affect the business. And there should be a detailed risk assessment which helps to identify the system vulnerabilities, threat, and current controls and attempt to determine the risk based on the likelihood and threat impact.

By applying a properly planned risk assessment helps to identify risks related to business critical

applications and will help to develop recovery strategies during business disruptions.

4.2.3 IT Inventory

Information is documented for all mission critical applications, said the IT infrastructure Manager, *which includes, Server Name, IP Address, physical host, virtual host, storage, processor, Memory and description of each server are documented and also configuration information is documented related to mission critical applications, from application side source code, user guideline, URL, Port number, Version and IIS configuration information as well as from system side documents Server Name, IP Address, physical host, virtual host, storage, processor, Memory and description of mission critical applications are documented.*

He added *mostly resources mapping to business critical applications, is based on resource allocation request initiated from application development team as per requirement to business critical applications, since most of business critical applications are developed in-house they use intensive resources.*

Property administration Manager said, *they perform all asset inventory of items annually including hardware & software and stock update inventory monthly* moreover, *IT infrastructure performs hardware & software inventory related to business critical applications and perform daily check on the systems.*

One of the steps in disaster recovery planning is Inventory, which mainly focused on hardware or software inventory of IT resources, when departments perform proper IT inventory, will help to manage the resource they have, they can even plan for what is required in the comping new implementation process. Moreover, will also help to identify resources mapping of existing business critical applications, improve resource utilization and helps to draw what is required for future plan.

4.2.4 IT Business Impact Analysis

After the risk assessment is completed, it will be used as an input to the business impact analysis. At this point, the interdependency of mission essential business applications is identified. According to data gathered from the Application Development Team Manager, *there is an undocumented interdependency between mission-critical business applications such as Warehouse, Central Depository, Membership, Trading Operation, Clearing and Settlement, active directory*

service, and database system applications. This study identified the interdependency of each business critical applications and documented in the architectural framework of Figure 4.1.

IT Security Manager stated, *until now they didn't conduct business impact analysis for mission critical applications, but Specific business unit conducts business interruption analysis such as (Warehouse, CD, CNS, Trade). As said major functional requirements for the business to functions or abilities must be present in order to continue business operations after a major (or minor) business disruption, includes Electrical and Mechanical parts of the datacenter functionality, Server and storage health and functionality, Application and Database functionality, Network and Connectivity functionality.*

BIA is a mandatory step to evaluate business processes and related IT systems to define the important functions that the system performs. And identifying the specific business processes and IT resources (hardware, network, software, and data) that are required to perform the task are identified and documented at this stage.

At this point, there should be a means to figure out the best time to recover the IT system by weighing the cost of system inoperability against the cost of resources needed to restore the system. Better crucially, creating a recovery priority that enables mission-critical systems make more educated, targeted decisions about contingency resource allocations and expenditures, saving time, effort, and money.

At this stage of the process, one can able to identify what are the critical business processes, RTO & RPO of those critical applications, dependency of mapping of processes, prioritizing which process to recover first, and which will be next, giving sequence and also developing recovery strategies for those business critical application are the activities that will be done in this phase.

4.2.5 Recovery Strategies

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in contingency plan. The alternate site type may be categorized in terms of their operational readiness, the site may be identified as cold sites, warm sites, hot sites, and mirrored sites.

Further, the normal reason for taking backups and/or archiving is for future use, and the duration might be for short term or archiving. More importantly, there are a number of ways (modes) of taking copies or archiving data, which one is chosen depends on how the plan to recover, to what

point (RPO) and at what speed (RTO) to minimize the business impact of a major failure.

The system data should be backed up regularly, and the policy should specify the frequency of backup like daily, weekly, incremental or full based on data criticality and the frequency that new information is introduced.

Reply from IT Infrastructure Manager, stated that, *the frequency of taking backup of mission critical applications is daily for windows system state, exchange mail, for Database backup every hour, and application backup on weekly basic or when there is a change.*

Considering the order of recovery for business critical applications, to determine which applications should be restored first, as said *they examine mission-critical services for recovery by considering criticality, relevance, and sequence, among other factors. They prioritize the recovery of important applications like trading, clearing and settlement, central depository, surveillance, and membership applications as a first priority.*

As a data backup method, he said *for long time they have had been used windows backup and recovery solution for servers and Sql server backup solution for the databases. But currently they have purchased commercial backup solution that can handle the task effectively. Also they are on the process of purchasing backup appliance that can perform backup and recovery of systems and applications with a click of a button.*

Finally to show how the business would function in a backup recovery site, *he recommend first to identify what is needed in terms of staff, equipment, supplies, communications, processes, and procedures. Moreover, for proper DR site that should be configured by taking in to consideration geographic location, resources and staff and proper processes and procedures should be in place.*

Disaster recovery strategy allows recovering a business from disruption of planned or unplanned outage of system which is caused by technical errors or human made, even may be natural disaster. Therefore, having a properly organized and documented disaster recovery strategy help to restore the business back to normal operation before a disaster happens.

4.2.6 Disaster Recovery Plan

According to interview reply from IT Security Manager, *there are no policies and procedures for IT disaster recovery plan in place, currently they are on progress of preparing BCP plan by doing the Risk Assessment and BIA. But there are policies and procedures for routine usage of*

mission critical business applications like database, system and application recovery plan as well as backup data which are barely updated. There is a generalized IT Infrastructure policy and specific non organized procedures for mission critical business applications that are organizing in to a departmental level.

When a disaster strikes, firms without disaster recovery plans have an enormous challenge. If a company's core business processes are highly time-sensitive, it's almost guaranteed to fail. If a disaster strikes a company without a disaster recovery strategy, that company has a low chance of surviving. It's also far too late to start planning.

Understanding the phases of the disaster recovery plan, aids in the development of methods for managing activities if the plan must be implemented. Activation, disaster recovery, business continuity, and resumption of normal operations are the typical steps. Regardless of whether the strategy is ever implemented, it must be tested and maintained.

The IT Infrastructure Manager added that, considering existence of internal and external data or application dependencies, *there is no procedure to ensure all dependencies are addressed in the correct order and timing, but by discussing with the whole IT team and team from business users they draw dependencies.*

IT recovery plan contains a lot of potentially sensitive operational and personal data, its dissemination throughout the company should be labeled and controlled. The copy should be stored at an alternate site with backup media to ensure availability. Storing the copy at an alternate site ensures its availability and good condition in the event that local plan copies cannot be accessed due to a disaster. Other information that should be stored with the plan includes contract with vendors (SLA), software license, system user manuals, and so on.

The document should be assessed to verify that it has up-to-date information and that it is updated on a regular basis, because tracking the status of the recovery plan is difficult or impossible without the needed information, which makes management decision-making difficult.

4.2.7 Awareness

Training and testing are two closely related processes, with training focusing on informing team members about specific roles and responsibilities during the implementation of the DR plan. It should include training on the specific skills required to implement and manage the strategy effectively.

IT Security Manager stated, currently *there is no disaster recovery plan in place, they are in the*

process of drafting a disaster recovery plan policy and procedure. As a result, without generating the document, IT disaster recovery cannot be implemented until awareness, training, and practice have been completed.

He added that *all previous procedures should be followed thoughtfully and attentively before proceeding to this stage. The plans should be defined initially, followed by the organization of specific backup and recovery operations, as well as the development and testing of policies and procedures.*

The BC/DR training should also include cross-functional teamwork and communication. Training can help to increase the chances of succeeding in the long run. Defining the scope and objectives for disaster recovery and business continuity training, conducting a needs assessment (gap analysis), planning training, scheduling and delivering training, and monitoring/measuring training are all part of the process.

Team members are trained on how to use the plan, their unique roles and responsibilities, and how to communicate throughout the business by testing it. Testing the plan will also aid in identifying any processes, procedures, actions, or checklists that are inaccurate, have gaps, or require adjustment.

The plan is tested to ensure that the processes, procedures, and actions outlined are understood. It checks for task integration and dependencies across different business and functional units. It also aids in determining whether the appropriate resources for the various processes have been found. Finally, it familiarizes implementers with the complete process and identifies any gaps or errors.

4.2.8 Maintenance and Audit

As per discussion with IT Auditing Manager, *Risk based internal audit is conducted by internal audit department to help the risk management function of the company by providing assurance about the risk mitigation. And their main activity involves detail IT audit for asset management of hardware and software items which goes through from procurement up to disposal of products.*

He added that, *there is IT control auditing, using general control auditing of good governance, change management, using application control auditing of compatibility, business continuity, input control, process control, output control, access control.*

As said, *they have external security audit SLA which will be done annually by external entity (INSA), performing security auditing of System administration configuration, network*

configuration, application system performance and access control. Moreover, IT Infrastructure Manager added *there is SLA for Storage system maintainace and support service agreement 24/7 including delivery of spare parts. Hence there is no proper disaster recovery plan in place, no maintenance or update done on IT DRP, still it's under progress of development and he added that they identified the necessity of developing IT DRP plan document per the regulatory advice and enforcement.*

A procedure for monitoring and analyzing change requests is one of the tactics for managing change. It's usually easier to keep track of change over time and respond as needed. The BC/DR team should have a clear, consistent methodology for reviewing and incorporating change and merging to current processes when change requests are issued. An audit should be carried out as a routine project activity, with an audit plan being established. There will be a review of BC/DR plan test plans and activities, as well as a review of BC/DR plan training plans and activities.

4.3 Architectural Framework of Critical business applications

Figure 4.1 presents framework helps to identify the essential structures of critical business application, relationship that exist in between the different applications and the dependency mapping of each critical business applications.

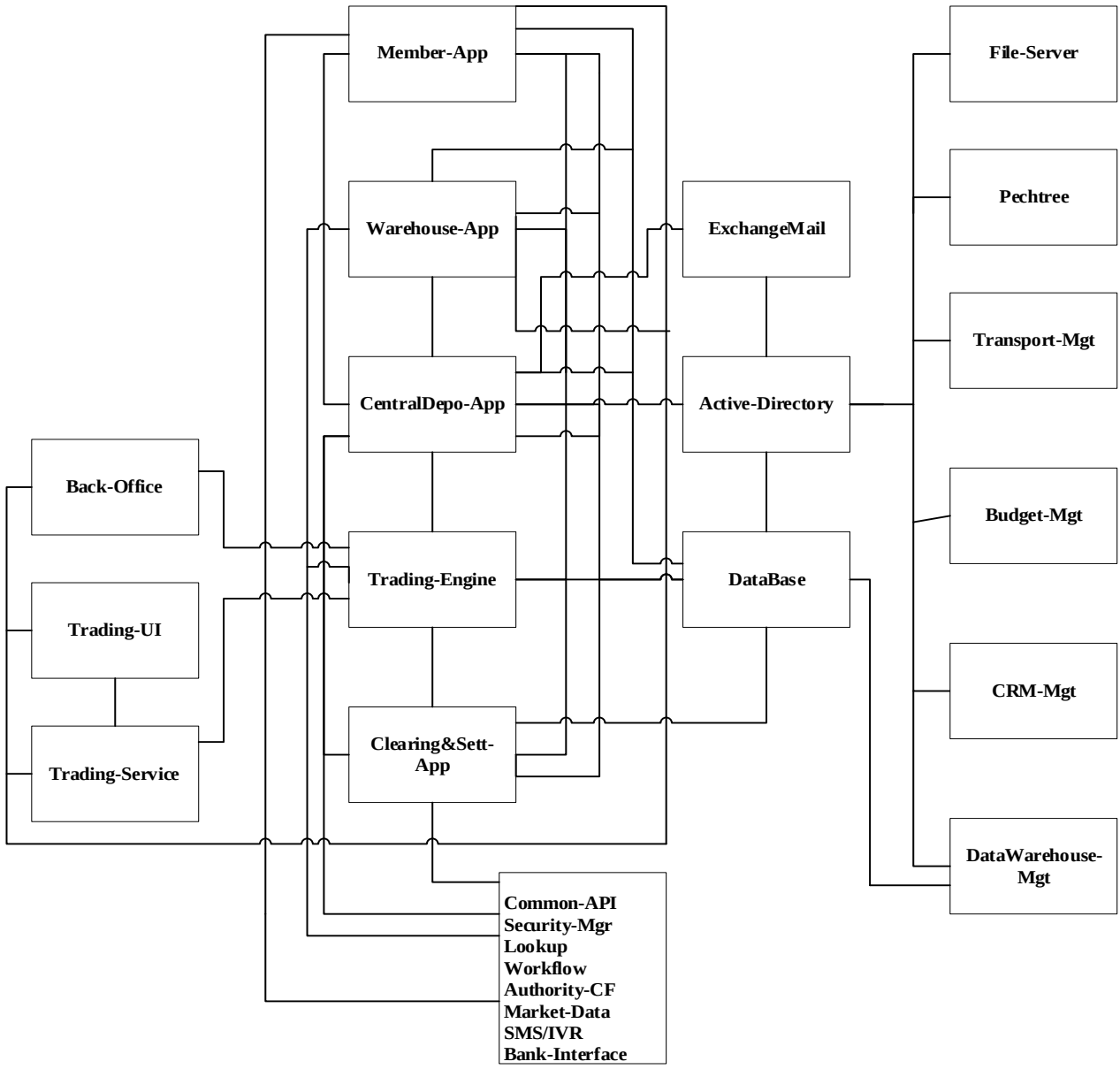

Figure 4.1 ECX-Business critical applications architectural framework

4.3.1 Architectural Framework of Trading Application

Business impact analysis is one of the most important activities that will be carried out during the disaster recovery planning process. Identifying core business applications and building dependency maps of such applications is one of the main activities during the business impact analysis phase.

Following the collection of data for this study and a thorough discussion with domain specialists, this study reach a conclusion of result and draw suggested framework as presented in Figure 4.2. And it was determined that all trading applications are heavily dependent on their subcomponents, as

well as active directory and database systems. Furthermore, at least one child domain active directory service and the principal database system must be operational for all trading applications to function properly.

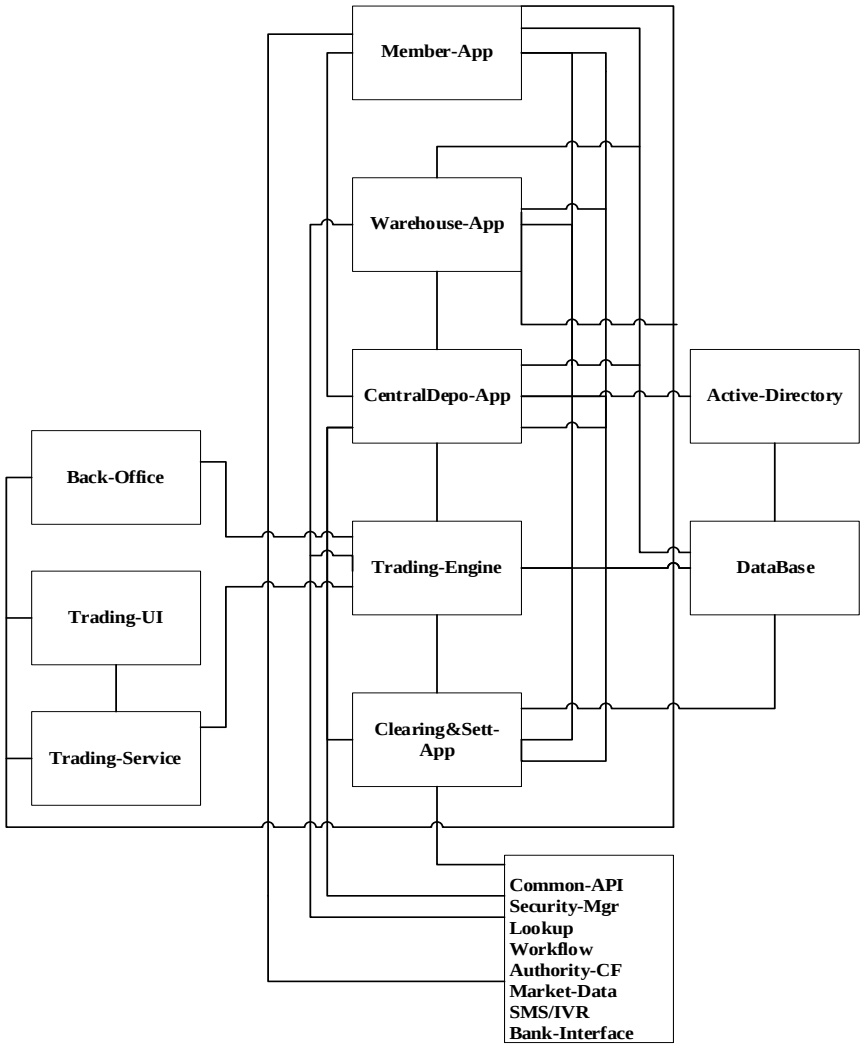

Figure 4.2 ECX-Business critical trading applications architectural framework

4.3.2 Architectural Framework of Operational and other Application

Other than trading applications, as presented in Figure4.3 this study identified that all the operational applications such as File server, Pechtree, Transport-Mgt, Budget-Mgt, CRM-Mgt, DataWarehouse-Mgt highly depend on active directory. Since the exchange mail service primary configuration and routine access of user emails depend on directory information service, the presence and proper functioning of active directory is mandatory.

Further DataWarehouse-Mgt contains historical data, and those data are from database system. Therefore, the proper functioning of database system is essential.

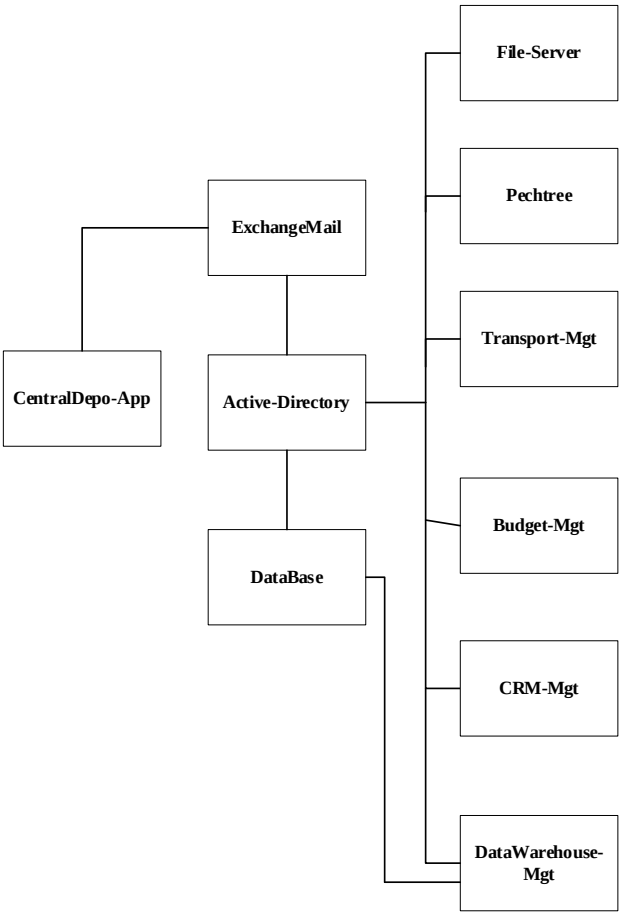

Figure 4.3 ECX-Business critical operational applications architectural framework

4.4 Disaster Recovery Strategy

Business processes can be brought back to normal operation by following a set of policies and procedures. As presented in Figure 4.4 which was adapted from the previous framework, show the sequence of activities to be performed after a disaster in order to restore a system outage.

To begin, risks related to critical business applications were identified during the risk assessment phase, critical business processes and recovery sequences for those applications were identified during the business impact analysis phase, BRP and DRP documents were created during the business continuity program design phase, and recovery priorities for business applications were created, during the develop recovery priorities phase, a recovery sequence for critical business processes will be created. Next, the IT strategy design stage will focus on high availability of systems, followed by the business resumption stage, which addresses how the business will resume after a catastrophic disaster. And final stage will be Implementation methodology which subdivided into four section and testing the performance in virtual environment.

At each stage of the process, during data collection of this study the framework were validated and at implementation stage of the research, experts in the field were advised to verify that really the proposed framework works for what this study try to achieve. Each steps further explained in the next section.

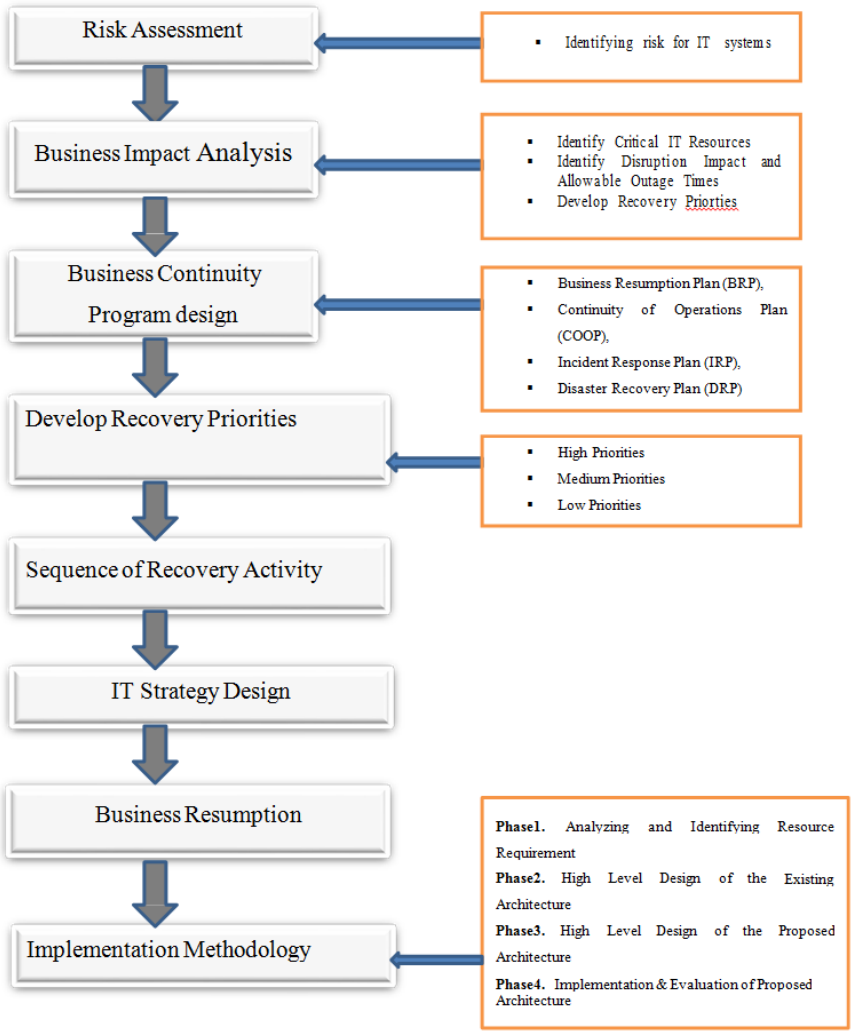

Figure 4.4 proposed framework of disaster recovery strategies

4.4.1 Risk Assessment

Risk assessment mainly focused on identification, analyzing, and evaluation of risks associated to a specific action or event to business application. The aim is to prevent business application security defects and reduce the likelihood of potential threats within an organizational business process. Contrarily the vulnerability assessment helps to analyze how vulnerable, susceptible, and exposed a business or system to a particular threat.

Using impact assessment analyzes how great or small the impact of a threat occurrence will be on the business or system and using Risk mitigation strategy development helps for deciding which risks should be addressed and in what manner. The inputs to this are the risk assessment analysis or reports, which delineate which threats exist, how vulnerable the systems are, and how

likely the threat is to occur as well as the impact of these occurrences on business.

4.4.2 Business Impact Analysis

Conducting a Business Impact Analysis is the process of identifying critical business activities or processes that the Contingency Planning Coordinator must carry out in order for the organization to achieve its most significant goals. These should be critical activities, processes, or systems without which the organization will either decline or lose its ability to pursue its goals successfully.

The first stage in performing a BIA is to identify business critical activities and/or processes that are critical to accomplishing organizational strategic objectives. Including interdependent processes crucial to attaining the objectives and during business processes is also an important part of describing the activities.

Other activities that should be addressed at this level include minimum resource needs for each process, Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO). Table 4.1 summarizes critical business application dependency mapping.

No.	Applications Type	Resource	Depends on Resource
1.	Active Directory Services	Active Directory Servers (AD) primary	Active Directory Servers(AD) Secondary
2.		Active Directory Servers (AD) secondary	Active Directory Servers (AD) primary
3.	Trading Application Services	Trading-Engine	Back-office, Trading- UI, Trading-Service, Database, Active Directory
4.		Membership-App	CentralDepo-App, Common-API, Database, Active Directory

5.		Warehouse-App	CentralDepo-App, Common-API, Database, Active Directory
6.		CentralDepo-App	Trading-Engine, Warehouse-App, Common-API, Database, Active
7.		Clearing&Sett-App	CentralDepo-App, Membership-App, Trading-Engine, Warehouse-App, Common-API,
8.		Common-API	Warehouse-App, CentralDepo-App, Clearing&Sett-App, Database, Active
9.	Database Application	Database	Active Directory Services
10.	Exchange Mail Service	Exchange Mail Service Primary	Active Directory Services
11.		Exchange Mail Service Primary	Active Directory Services
12.	Operational business applications	Peachtree Application Servers	Active Directory Services
13.		File Servers	Active Directory Services
14.		CRM Server	Active Directory Services
15.		Budget Management Server	Active Directory Services, Database Service

16.		Transport Management Server	Active Directory Services, Database Service
17		Data Warehousing Server	Active Directory Services, Database
18.		Remaining Application Servers	Active Directory Services

Table 4.1 Critical business application dependency mapping

Aside from identifying an organization's critical business functions and analyzing the potential disruptive impact to the business, the Business Impact Analysis phase also assesses the outage time of any functional area or business operations within the organization. And also determines the extent to which primarily functional & operational dependencies exist within the organization, and establish the restoration priorities & sequence of the critical IT applications. Figure 4.5 depict the Business impact analysis of critical business applications, and will be used as an input to implementation method for this study.

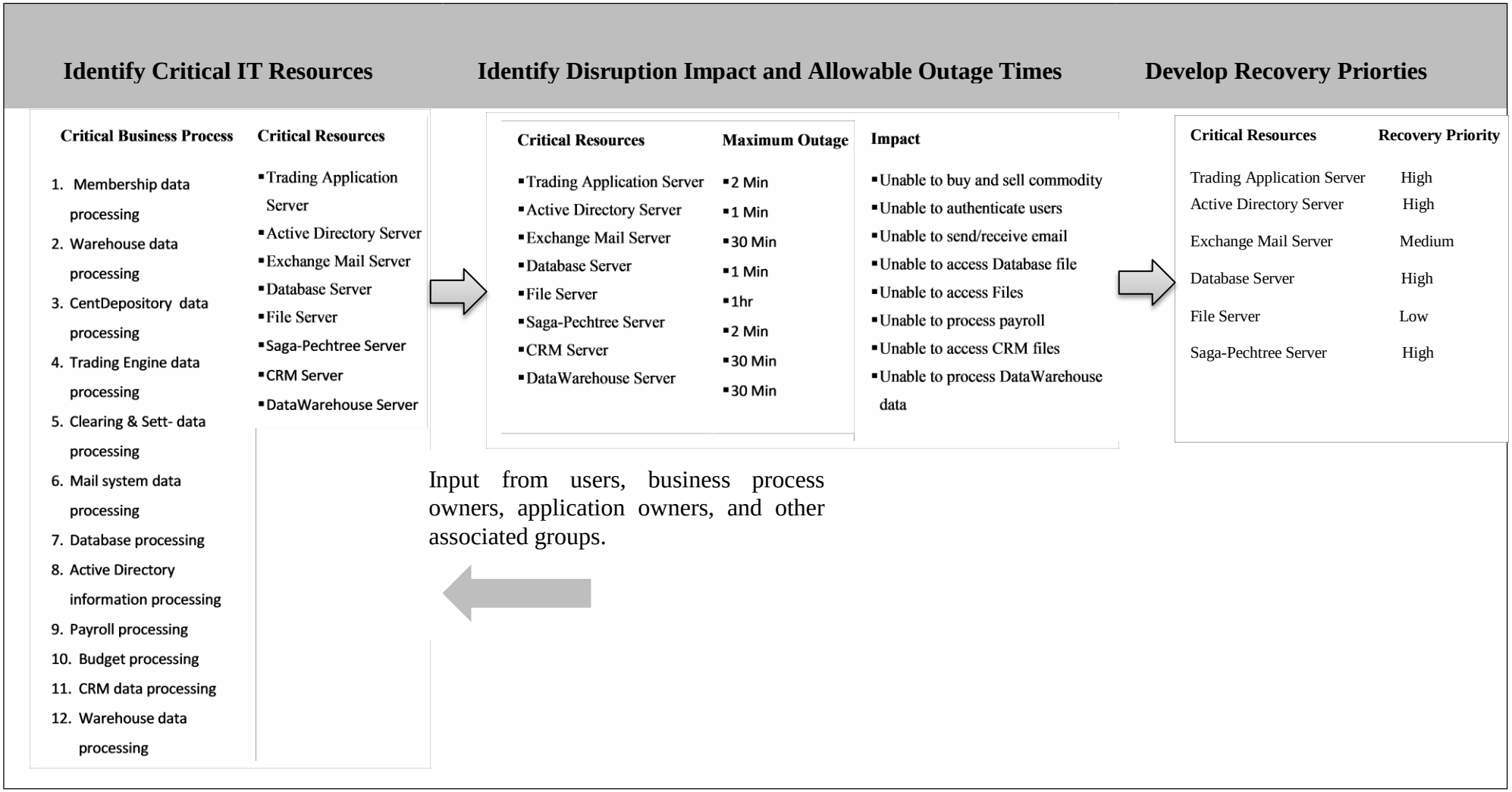

Figure 4.5 Business impact analyses of critical business applications.

4.4.3 Business Continuity Program Design

In this phase of recovery strategy, design or enhance the existing end-to-end Business Continuity program will be done, including preparation of procedures for:

- Business processes and procedures (non-IT)
- Crisis team management (IT and non-IT)
- Definitions of how non-IT portions of the business will resume operation
- The external, non-IT business process aspects of High Availability and Disaster Recovery And recovery plans in all aspect like:
  - Business Resumption Plan (BRP), mainly on restoration of business processes after an emergency.
  - Continuity of Operations Plan (COOP), for restoring an organization's (usually the headquarters element) essential functions at an alternate site.
  - Incident Response Plan (IRP), establishes procedures to address cyber-attacks against an organization's IT server and workstation systems.
  - Disaster Recovery Plan (DRP), a plan designed to restore operability of the target system, application, data, or computer facility at an alternate site after an emergency.
  - Establishing Crisis management and Top management team

4.4.4 Develop recovery priorities

The outage impact(s) and allowable outage times characterized in the previous step enable to develop and prioritize recovery strategies as presented in Table 4.2 that will implement during contingency plan activation. For example, if the outage impacts step determines that the system must be recovered within 4 hours, the Contingency Planning Coordinator would need to adopt measures to meet that requirement. Similarly, if most system components could tolerate a 24-hour outage but a critical component could be unavailable for only 8 hours, the Contingency Planning Coordinator would prioritize the necessary resources for the critical component. prioritizing these recovery strategies, will make us more informed, tailored decisions regarding contingency resource allocations and expenditures, saving time, effort, and costs. During data collection of this study identified that, business critical applications prioritized as follows in Table 4.2. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational

capabilities over a longer recovery period.

No.	Resource	Recovery Priority
1.	Active Directory Servers (AD)	High
2.	Trading Application Servers	High
3.	Exchange Mail Servers	High
4.	Peachtree Application Servers	High
5.	File Servers	Low
6.	CRM Server	Medium
7.	Budget Management Server	Medium
8.	Transport Management Server	Medium
9.	Data Warehousing Server	Medium
10.	Remaining Application Servers	Low

Table 4.2 Business critical applications priority

4.4.5 Sequence of Recovery Activity

Recovery processes for a complex system, such as an online trading platform with several separate components, should be based on the system priorities indicated in the BIA. To avoid substantial impacts on linked systems and their applications, the sequence of activities should mirror the system's authorized outage period.

Because this study does not cover the creation of recovery processes document, but suggest that the procedures should be described in a step-by-step, sequential structure, with system components restored in a logical order. If a LAN is being restored after a disruption, for example, the most vital servers should be restored first, followed by less critical servers such as file servers.

Similarly, in order to recover an application server, first restore and verify the operating system before recovering the program and its data. When particular scenarios arise, the processes should also include guidance on how to coordinate with other teams.

If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured. These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and

vital records for recovery of the system.

4.4.6 IT Strategy Design

At this stage, high availability of systems should be addressed. When we say a system is high available, it means that the system will be available most of the time. Without high availability of Server, it's not possible to create high available application system. This study identified that, in existing production site, IT infrastructure is highly available like network connectivity, AC, Ups, power supplies, storage systems.

4.4.7 Business Resumption

When a disaster happen we need to plan with recovery strategies that provide how to restore IT operations quickly and effectively following a service disruption. At this stage of disaster recovery strategy, identification of critical business followed by how they are going to be resumed to previous operation before a disaster occurs will be the main activity.

4.5 Implementation Methodology (System Built)

One of the main tasks of applying Design science research is improving the performance of a system by designing and evaluation of artifacts, artifacts could be method or a model. At this stage, this study divides the implementation of the system architecture in to four phases shown in Figure 4.4. Phase1. Analyzing and Identifying Resource Requirement, Phase2 High Level Designs of the Existing Architectures, Phase3 High Level Designs of the Proposed Architectures, and Phase4 Implementation and Evaluation of Proposed Architectures.

4.5.1 Phase1. Analyzing and Identifying Resource Requirement

Phase1 mainly focused on comprehensive study of Server virtualizations and resource sharing. It is identified that, virtual server environment component will be used in the implementation as part of DR site. VM is a robust soft partitioning as well as virtualization technologies that gives operating systems isolation, distributed CPU (along with sub-CPU granularity), distributed I/O, and automatic, dynamic resource allocation that is built in. The physical resources of the server are shared amongst any of the VMs it hosts, based on demand and entitlement. Each VM hosts its own applications in a fully isolated environment. The VSE for servers is an integrated virtualization solution for the server environment.

4.5.2 Phase2. High Level Design of the Existing Architecture

In this phase identification of existing environment will be done, which includes interconnection of high end blade servers and storage system. During data collection of this study, it is identified that the existing environment consists of physical servers with virtualization of using Hyper-V and VMware as presented in Figure 4.6. The virtual infrastructure consists of two virtualization hosts (or physical servers) in separate Rack with Storage Area Network (SAN) to storage system. While the virtual machines are created with different installed operating system and application programs, all necessary resources like number of processor, memory, network port are allocated in the shared environment.

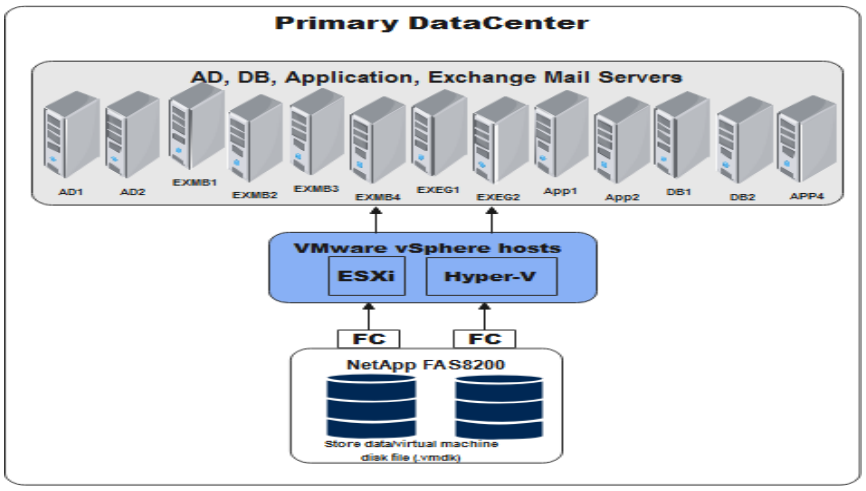

Figure 4.6 existing architecture of critical business applications

Each virtual machine consists of multiple allocated disks from the storage system, and those disks classified as primary and secondary disks. Primary disks are mainly used for operating system and application program installation, and secondary disks are used for purpose of data store. Moreover, as stated each business critical applications installed and configured accordingly with the required configuration

4.5.3 Existing Active Directory Architecture

Active Directory is a repository location where it stores information about, user accounts, computer accounts, security groups, organizational units, and other directory objects. And also it helps to manage tasks as creating, configuring, maintaining, monitoring, and deleting user accounts, groups, computer accounts, and other directory objects.

As shown in Figure4.7, the existing active directory infrastructure contains one primary domain controller and one secondary domain controller for staff. And one primary and one secondary child domain controller for traders. The active directory information is replicated from primary domain controller to secondary domain controller and from root domain to child domain controllers vice versa.

During business hour users are authenticated from root and child primary domain controllers. If the primary domain controller is down, all the traffic is redirected to secondary domain controllers. Therefore, unless there is a whole datacenter down, the service is available all the time.

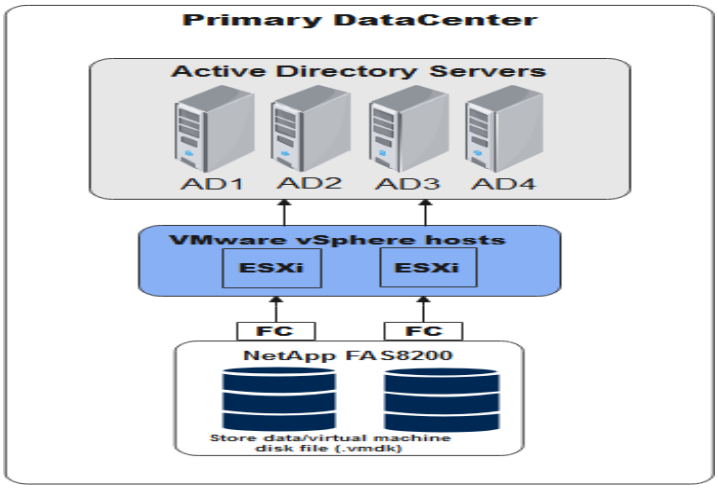

Figure 4.7 Active Directory service architecture

For disaster recovery, all system state and full data backup is taken every day and manually copied to disaster recovery site server. Whenever there is system crush in the primary datacenter, backups will be taken from DR site and restored to primary site. And currently there is an offsite backup location and is considered as disaster recovery site, it's a cold disaster recovery site.

4.5.4 Existing Exchange Mail Service Architecture

Email is one of the most visible services that, most organizations have become dependent on. And use this soft information to run their business. As a result, users have developed an attachment to email system. Microsoft's Exchange Server products play a key role in electronic messaging or email system.

The exchange mail service deployed in the existing environment is Exchange Server 2019. And the exchange server 2019 has two roles, exchange server mailbox and exchange server edge

roles. Exchange mailbox role which holds user emails and exchange server edge role, mainly involved in email transportation and filtering.

Figure 4.8 presents one primary mailbox and one secondary mailbox for staff, each of which hosts five mailboxes. And additionally there is one primary mailbox and one secondary mailbox for traders, each of which hosts two mailboxes. Edge Primary and Edge-Secondary help to route email from within the mailbox server to other mailbox servers and to the internet.

In addition to role configuration, there is also DAG (database availability group) configuration, helps availability of mailbox servers when system unavailability happens in one of mailbox server. DAG with windows failover configuration implemented in the existing environment which helps to redirect traffic from failed server to available server when system interruption happens in both case configurations.

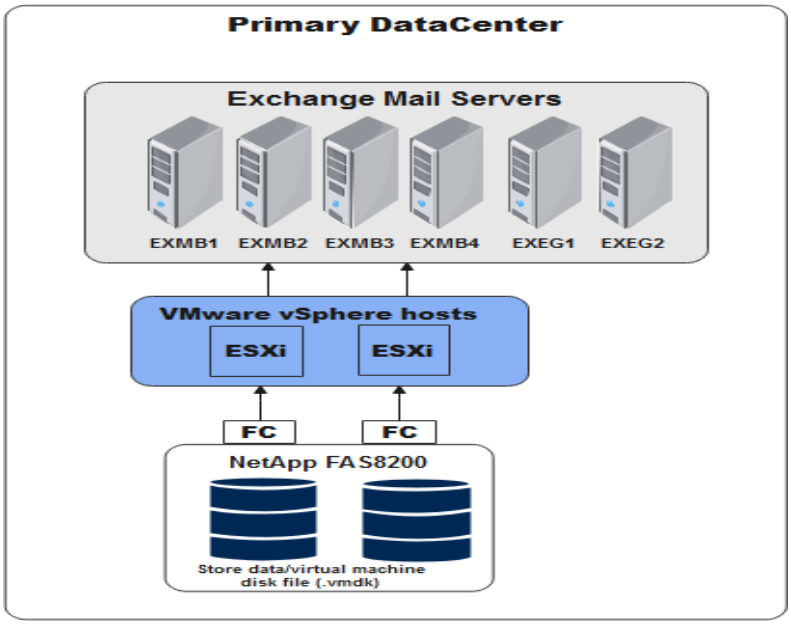

Figure 4.8 Exchange server mail service architecture

Exchange Server stores all configuration and recipient information in the Active Directory service database, and when an Exchange server requires information about recipients from the configuration of the Exchange organization, it queries Active Directory. Active Directory servers must be available for Exchange to function correctly, in this case primary active directory server should be available or both.

In case for disaster recovery, system state, mailbox data and full configuration information is backup using offline storage media like external disks and manually copied to DR site server. And when a system crush happens in primary site, those back data are copied from DR site and restored in production site.

4.5.5 Existing Database Architecture

For high availability of Database system, mirroring is configured within the primary data center as shown in the Figure 4.9. To achieve database failover, asynchronous database mirroring with no witness SQL Server instance is configured. When zero data loss is required, the database mirroring high-safety mode (asynchronous) setting is enabled to achieve less data loss between the two servers located in the primary data center.

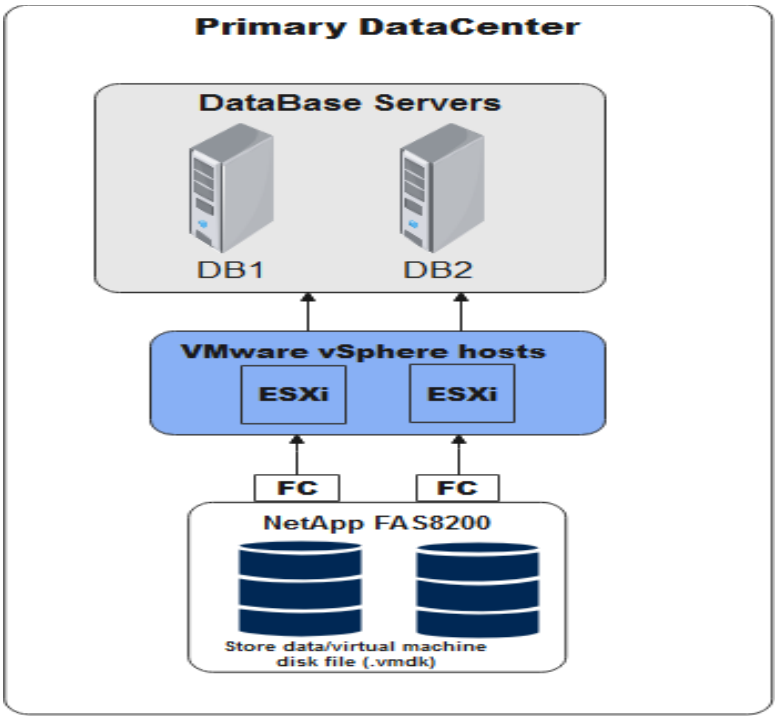

Figure 4.9 Database service architecture

Since the Production DB and Mirrored DB servers are located in different Rack, Mirroring operating mode, high performance (asynchronous) commit change at the production, primary DB and then transfer them to the mirroredDB. DB Mirroring occurs every day, every 5 min. Moreover, the transactional log backups occurs every 30 min and full back up occur every day, then the full backup is moved to the DR Server and then restored every day.

4.5.6 Existing Trading Business Critical Application Architecture

Figure4.10 summarizes flow of data between different applications layers, all the codes are published in IIS. Front office application inserts data for trade readiness using trading-service. When trade data are ready and sessions opens, trade order will be inserted from UI form, UI sends order data to services then trade UI service saves the data to message queue for trade engine. Trade engine service reads the data from message queue and send to trade engine, trade

engine validate the order save the result to database. Trade UI Service reads the data from database and sends the result to trade UI, trade UI finally display the result to users.

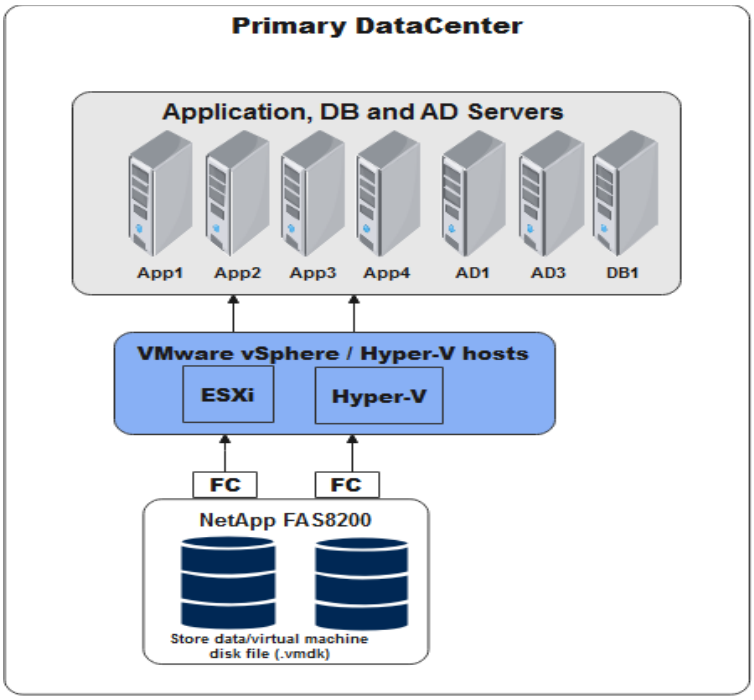

Figure 4.10 Trading business critical application service architecture

For disaster recovery, all the application source code, system state of servers, and full backup is taken using offline storage disks and when a system crush happens backups are restored.

4.5.7 Existing Operational Department Business Critical Applications Architecture

As shown in Figure 4.11, the different operational business critical applications are summarized below.

Customer Relationship Management (CRM) is an application software for managing all the company's relationships and interactions with customers and potential customers.

Saga-Peachtree is an accounting application that enables comptrollers and managers to automate and manage numerous accounting tasks, like: reconciling accounts payable and receivable, Creating financial statements, check invoices, detailed profitability tracking, cash flow forecasting and custom reporting.

Budget-Management is an application software used by finance Department for managing budget allocation used by different divisions for annual budget plan including purchasing of goods and services.

Transport-Management system, is an application software used by Transport service division to manage transport cars, which cars are available, which cars are in duty, available driver,

destination management of cars, fuel consumption of cars, and service time of cars.

Data-Warehouse- Management is application software, which stores current and historical data into one place for creating analytical reports. The goal is to derive profitable insights from collected data.

File-Server is used for creating, sharing of user Department files and storing archive data from all departments and divisions.

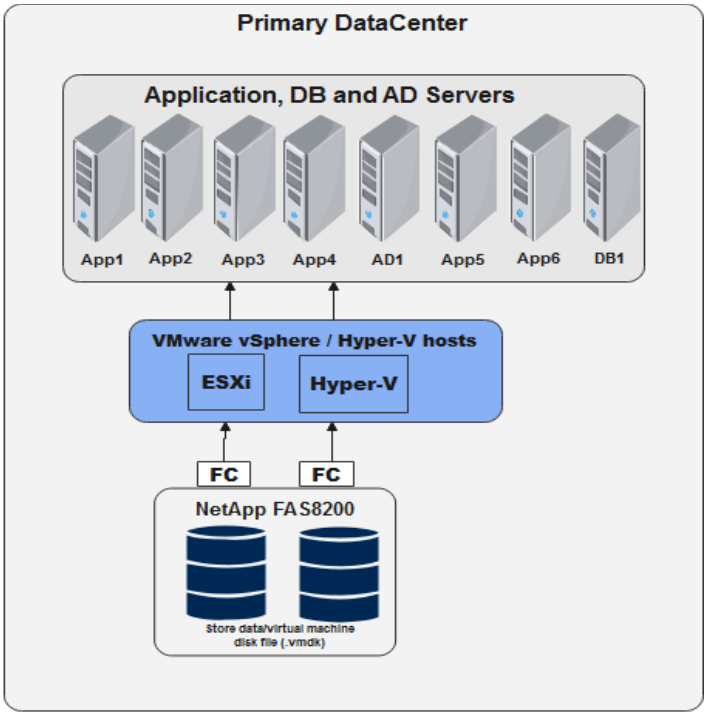

Figure 4.11 Operational business critical application service architecture

As a solution to disaster recovery, all system state configuration and full backup data of servers are taken using external disks and copied to DR site server. When a system crush happens, backups are copied from DR site to primary site and restored accordingly.

4.5.8 Phase3. High Level Design of the Proposed Architecture

4.5.8.1 The proposed Active Directory Architecture

Since active directory stores information about users, computers, servers, groups, etc and when the active directory unavailable in the primary site, users or devices will not be authenticated. Therefore, installing and configuring additional domain controllers from primary domain controllers of Staff and Traders, will help to allow authentication of users from DR site.

The two additional domain controllers configured in DR site will replicate in every 5 second, and

when there is total unavailability of active directory in primary site users can be authenticated from DR Site. Moreover, when Active directory server is crushed in primary site, will be reconfigured from DR site.

To handle redirection of traffic between primary site and disaster recover site, a DNS round robin will be configured. Round robin load balancing is done within an A record, by assigning multiple IP addresses to the same host. The DNS client tries the first IP address, and if it does not respond, waits 30 seconds for a timeout, and then tries the next address in the list, in this way traffic will be redirected as shown in Figure 4.12.

During system unavailability of Active directory information in production environment, users' traffic will be redirected to one of the available AD server in DR site. Moreover, if there systems crush in production site, will be recovered from DR site, because everything in production site is replicated to disaster recovery site every 3 second.

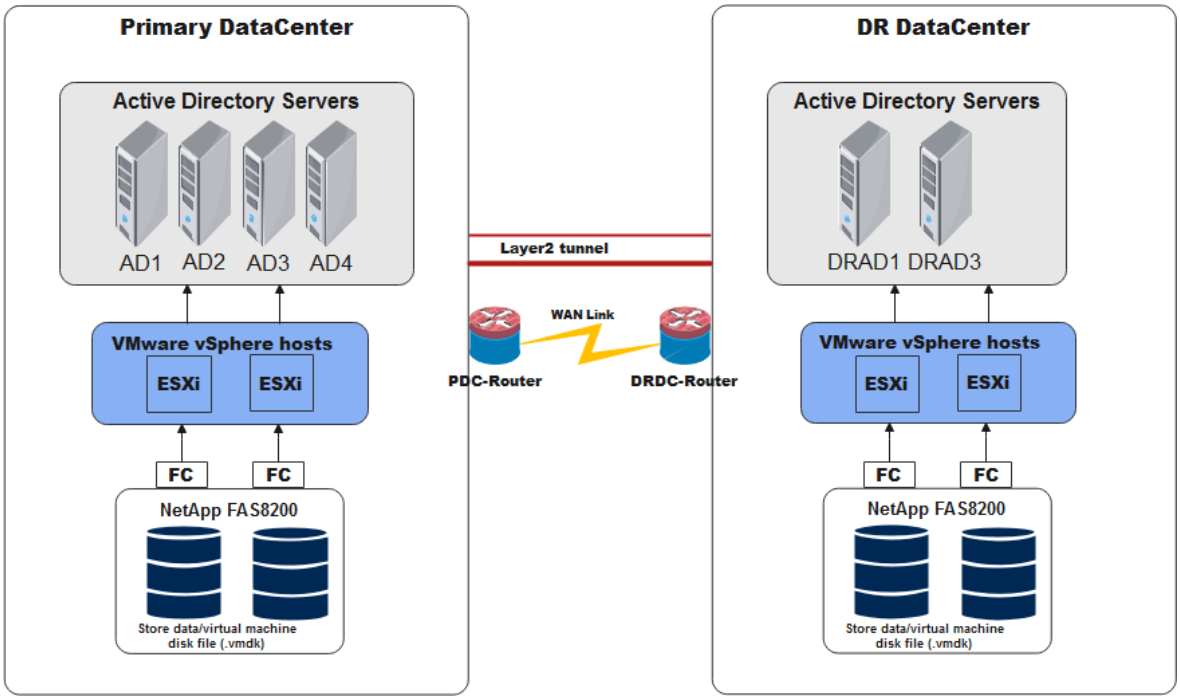

Figure 4.12 Proposed Active Directory service primary to DR site replication architecture

4.5.8.2 The proposed Exchange Mail Service Architecture

In the primary datacenter four mailbox servers are available as shown in Figure 4.13, two mailbox servers for Staff and two mailbox servers for Traders. And also DAG1 is configured with windows failover for Staff, and DAG2 configured with windows failover for Trades. When mailbox server unavailability happens in one of member mailbox servers, the traffic redirected

from failed server to working server.

In Disaster recovery site, Database Availability Group (DRDAG) will be configured, and one mailbox server from each Staff and Traders installed and configured in DR site and also these two servers should be member of DRDAG. To create replication of data, the two primary mailbox database server from the primary site also should be member of DRDAG. Therefore, with application layer replication between mailbox servers, all servers will have the same mailbox data. If all the mailbox servers in primary site unavailable, the traffic will be redirected to mailbox servers in DR site. And when there is a system crush in the primary site mailbox servers could be reconfigured from DR site mailbox.

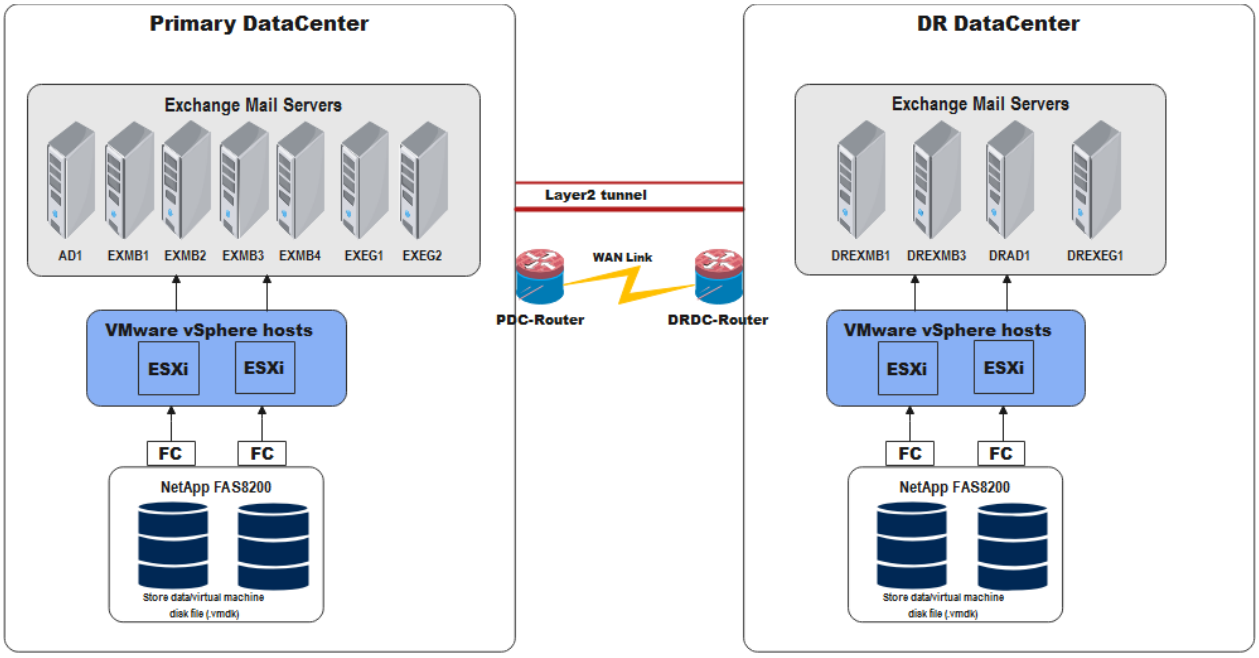

Figure 4.13 Proposed architecture of Exchange Mail Servers Replication system.

Since two Edge servers configured in primary site, traffic will be directed in one of the two Edge servers. In DR site considering resource utilization, one Edge server is configured and if in the primary site all mailbox server are unavailable, all the traffic will be redirected to DR site through DREdge server, DREXEG1 shown in the Figure. Since DNS round robin is configured as a load balancer for traffic management. Exchange Server store all configuration and recipient information in the Active Directory service database and the Active Directory servers must be available for Exchange to function correctly, in this case primary active directory servers configured in DR, DRAD1 should be available.

4.5.8.3 The proposed Trading Application Service Architecture

The two primary active directory servers configured on the DR site should be available because all trading applications highly depend on active directory servers. Considering resource planning for trading application configuration, the exact copy of the configuration of all trading servers should be available on the DR site as shown in Figure 4.14.

Since real time data access for trading applications is mandatory. Therefore, availability of database server in DR site should be a must and the data present in the database has to be real time data, this issue will be addressed by the proposed database architecture implementation in DR site.

Hence all trading applications are published on IIS 6, to create a high available disaster recovery of applications from DR site, this study propose a failover clustering for high availability & load balancing between servers and DFS replication for replication of source code data between the servers.

If the primary application server is down due to maintenance or system crush, all user traffic is diverted to the DR site's secondary application server. As a result, anytime one of the trading servers is down, the user's request traffic is forwarded to the next accessible server.

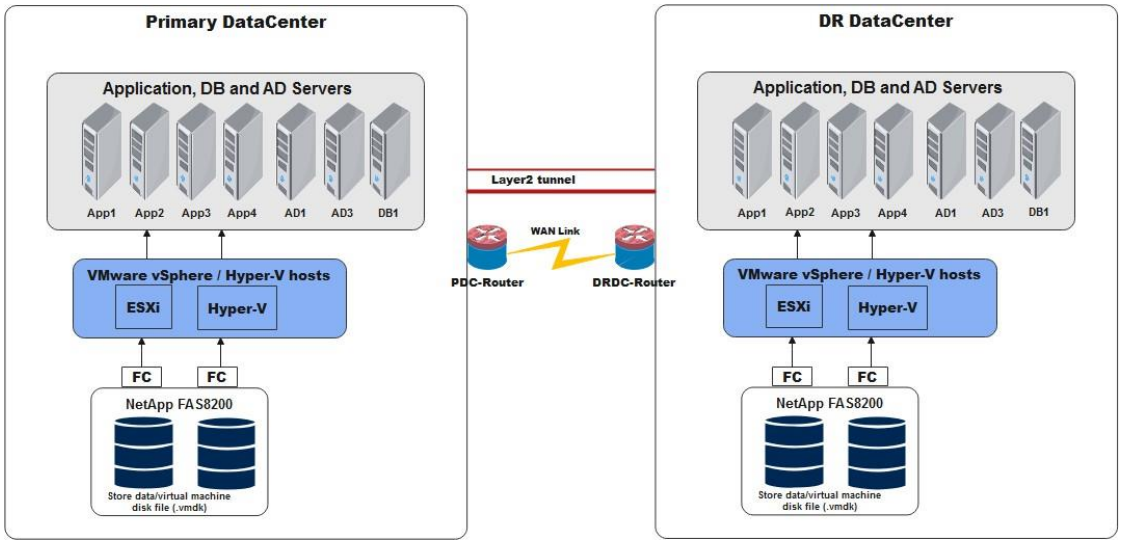

Figure 4.14 Proposed architecture of Trading Application Servers Replication system.

4.5.8.4 The proposed Operational Application Service Architecture

Figure 4.15 depicts the budget-management, transport-management, and Data-Warehouse-management applications are web-based applications published on IIS 6. Therefore, to create high availability of application servers, and disaster recovery of applications from the DR site, failover clustering & load balancing between servers for high availability and DFS replication

for the purpose of replication of source code data between the servers are used.

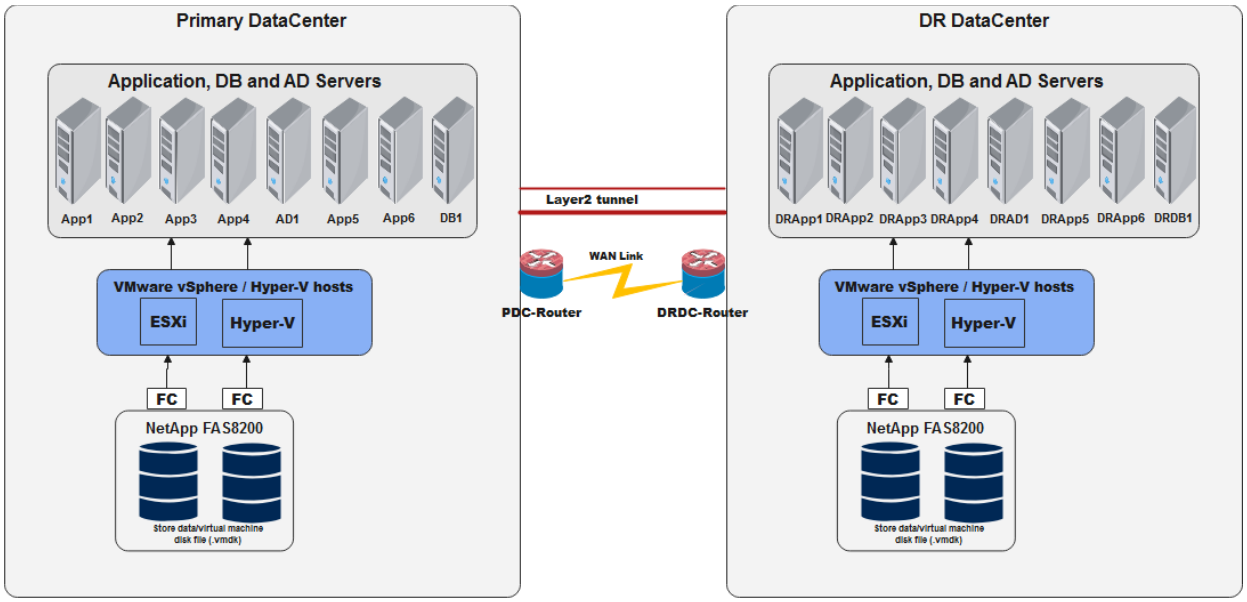

Figure 4.15 Proposed architecture of Operational Application Service Architecture

The Customer Relationship Management (CRM), Saga-Peachtree, File-Server, the applications are running in different platform of windows and Linux. Therefore, to create a high availability of service, this study propose a Veeam backup and replication method it performs image-based VMware replication with compression, deduplication and changed block tracking (CBT) technologies, which reduce traffic and speed up data transfer.

The mechanism of Veeam's VMware replication is similar to forward incremental backup. During the first job run, Veeam Backup & Replication creates a full virtual machine copy and then catches only the VM changes during subsequent job runs. This method is not an application layer replication and recovery way, it performs creating of replica Virtual Machine. And when a disaster happen, those backup will be restored from DR site. Moreover, by activating those replica VMs in DR site, user's traffic could be managed from DR site.

4.5.8.5 The proposed Database Service Architecture

Considering existing SQL Server architecture as presented in Figure 4.16, in primary datacenter the installed SQL Database system is SQL server 2008 R2, as a solution to high availability and disaster recovery, this study propose Failover Clustering for High Availability and Database Mirroring for Disaster Recovery.

In this architecture, failover clustering provides the local high availability and database mirroring provides the disaster recovery capability. A failover cluster on its own protects

against physical server, Windows Server, and SQL Server failures and Database mirroring is one way to provide a redundant copy of a single database on a separate physical server. A typical implementation of this architecture involves a failover cluster in the primary data center with database mirroring to a secondary data center or disaster- recovery site.

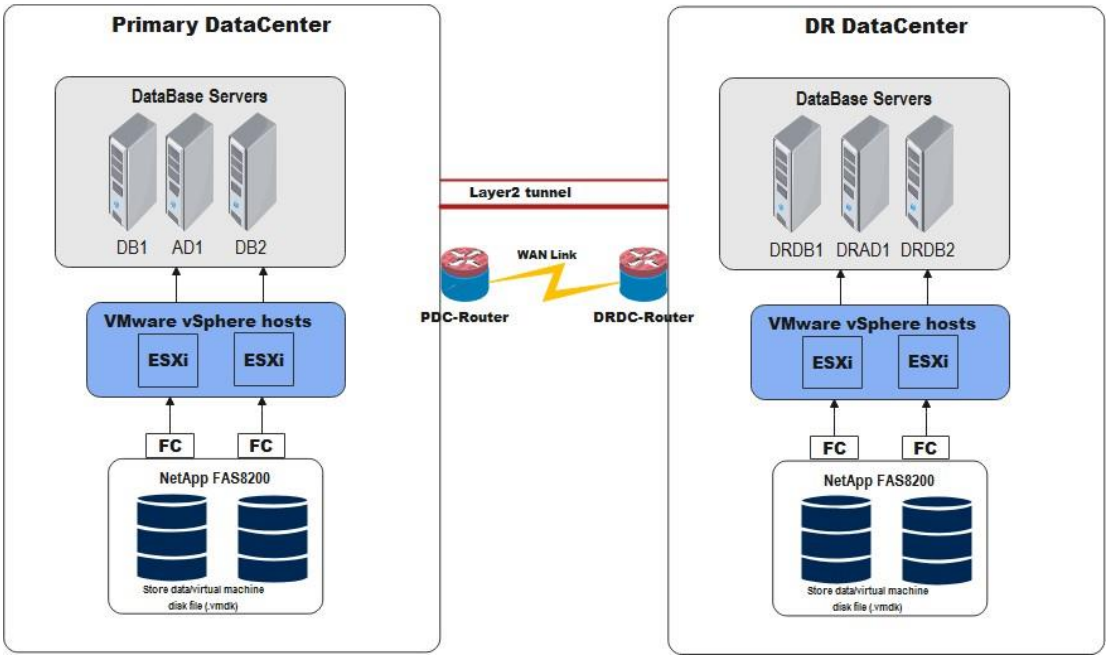

Figure 4.16 Proposed architecture of Database Service Application Architecture

The selected database mirroring for this study is Synchronous database mirroring, which can allow a zero data-loss requirement to be met, potentially with some workload performance impact depending on the type of workload and the network bandwidth between the two data centers. Asynchronous database mirroring does not guarantee zero data loss in the case of a disaster, but has no impact on workload performance and this study doesn't consider this.

4.5.9 Phase4. Implementation of Proposed Architecture

4.5.9.1 Production Site

In the simulation of the Production Site, this research uses VMware vSphere 7 as the virtual infrastructure for all architectures. The virtual infrastructure consists of two virtualization hosts (or physical servers) with a Storage Area Network (SAN) of NetApp storage as presented in table 4.3. The SAN is really a storage equipment for servers, so the servers are connected to the storage system, with attached to disks locally connected to virtual machines and the operating systems installed in the virtual machines.

4.5.9.2 Capacity Planning for Production Site

Capacity planning for virtual infrastructure has been conducted for production site implementation. This research has to make sure capacity planning for virtual infrastructure is being done precisely and effectively. A successful Virtual Infrastructure deployment is preceded by a Basic Consolidation Estimate (BCE), where existing IT infrastructure information collected from during interview and system administration document, as well as immediate future IT requirements will be assessed with the focus to better design a Virtual Infrastructure in the direction of specific IT and business goals. The actual VMware BCE is made to supply present environment's virtualization possible by providing an accurate assessment of Windows.

No.	Machine	# of Processors	Processer Type	Total Memory	NIC Ports	Internal Hard disk	Connector SAN
1.	ESXi-7 standard (VMware, Inc.)	2	16 CPUs x Intel(R) Xeon(R) Gold 6134 CPU @ 3.20GHz	512 GB	4	6TB	FC Port x 4
2.	ESXi-7 standard (VMware, Inc.)	2	16 CPUs x Intel(R) Xeon(R) Gold 6134 CPU @ 3.20GHz	512 GB	4	6TB	FC Port x 4

Table 4.3 Virtual Machine Specification for the Simulation Architectures

4.5.9.3 Capacity Planning for Disaster Recovery Site

Simulation of DR Site is identical as, the one for simulating the Production Site. Identical hardware configuration with required system resource and setup of application software are used to provide a seamless and bare-metal recovery for the virtual machine OS. Bare-metal restore is a method in the field of data retrieval and restoration where the copied data is accessible in a form that enables one to recover a computer system from "bare metal", i.e without the specifications concerning earlier installed software or operating system.

Type	CPU	OS	Memory	Hard Disk	Application	Database
AD1	4	Windows 2019	8GB	150 GB	Active Directory	No
AD2	4	Windows 2019	8GB	150 GB	Active Directory	No
EXMB1	12	Windows	32 GB	250GB	Exchange Server	No

		2019				
EXMB2	12	Windows 2019	32 GB	250GB	Exchange Server	No
EXEDG	12	Windows 2019	32 GB	250GB	Exchange Server	No
DB1	12	Windows 2008	32 GB	120 GB	IIS Web Server 6	MsSQL2008
DB2	12	Windows 2008	32 GB	120 GB	IIS Web Server 6	MsSQL2008
App1	8	Windows 2008	12 GB	120 GB	IIS Web Server 6	MsSQL2008
App2	8	Windows 2008	12 GB	120 GB	IIS Web Server 6	MsSQL2008

Table 4.4 Virtual Machine Specification for the Simulation Architectures

4.5.9.4 Experimental setup and tests (Evaluation of Systems)

Aside from system built, design science research involves evaluation of artifacts, This section discuss about testing implementation features of this project, the features described hardware and software configuration with necessary figures and will be configured the servers or nodes as follows:

No.	Host-Names	IP	URL	Description
1.	AD1.local.com.et	10.1.5.70		Active Directory Server1
2.	AD3.local.com.et	10.1.5.80		Active Directory Server2
3.	EXMB1.local.com.et	10.1.5.71	https://exmbx1.local.com.et and https://mail.local.com.et/	Exchange Mailbox Server1
4.	EXMB2.local.com.et	10.1.5.81	https://exmbx2.local.com.et and	Exchange Mailbox

			https://mail.local.com.et/	Server2
5.	EXEDG.local.com.et	10.1.5.85		Exchange Mail Edge Server
6.	App1.local.com.et	10.1.5.73	http://App1.local.com.et	Application Server
7.	App2.local.com.et	10.1.5.83	http://App2.local.com.et	Application Server
8.	DB1.local.com.et	10.1.5.72		Database Server
9.	DB2.local.com.et	10.1.5.84		Database Server

Table 4.5 Hostname and IP addresses of business critical applications

4.5.9.5 Installation and Configuration of Active Directory Server

Before starting to configure other application services, it's mandatory to install and configure the active directory server AD1. The first step in the installation and configuration of the active directory service is installing Windows server 2019 in AD1 and configuring the Active Directory Domain Service. And then assign IP addresses based on Table4.5 and create sample organizational units, users, and groups.

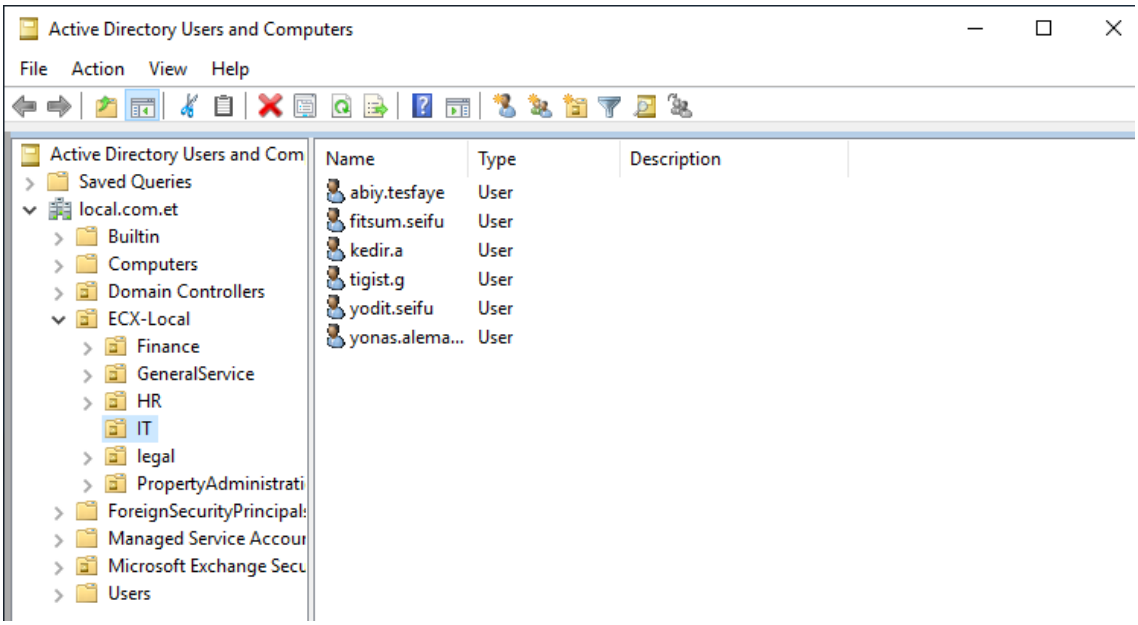

Figure 4.17 Installations and Configuration of Active Directory Server

Following the configuration of the first domain controller, an additional domain controller will be configured to balance the load and increase fault tolerance.

Once the two domain controllers on the primary site and DR site are configured, the next step will be testing the end to end connection between the two servers from, AD1 to AD3 and from AD3 to AD1, as shown in Figure 4.18. And from the test results, the two domain controllers have an end to-end connection and working properly.

```
PS C:\Windows\system32> ping 10.1.5.70 -n 2

Pinging 10.1.5.70 with 32 bytes of data:
Reply from 10.1.5.70: bytes=32 time<1ms TTL=128
Reply from 10.1.5.70: bytes=32 time<1ms TTL=128
```

Figure 4.18 ping test result of active directory server AD1

```
PS C:\Windows\system32> ping 10.1.5.80 -n 2

Pinging 10.1.5.80 with 32 bytes of data:
Reply from 10.1.5.80: bytes=32 time<1ms TTL=128
Reply from 10.1.5.80: bytes=32 time<1ms TTL=128
```

Figure 4.19 ping test result of active directory server AD3

From the results above, the next step is testing replication of directory information between the two active directory servers. While the two servers have the same active directory information, it means that they are replicating properly. As shown in Figure 4.20, the two servers are replicating. And from the results, the longest replication gap among the domain controllers is 5minute and the total replication is 5 with no error and no percentage of failure.

```
PS C:\Windows\system32> repadmin /replsummary
Replication Summary Start Time: 2021-05-20 07:49:51

Beginning data collection for replication summary, this may take awhile
  .....


Source DSA          largest delta    fails/total %%   error
 AD1                    04m:50s    0 /   5    0
 AD3                    03m:40s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 AD1                    03m:40s    0 /   5    0
 AD3                    05m:19s    0 /   5    0
```

Figure 4.20 replication status of active directory servers AD1 and AD2

Largest delta denotes the longest replication gap amongst all replication links for domain controller.

Total is the replica links for a particular domain controller.

Fail is the total number of replica links failing.

Percentage is the percentage of failures in relation to the total replica links on the domain controller.

Once replication between two domain controllers are working properly, next step will be checking if primary domain controller AD1 is down and AD3 is running and then testing users are able to login using AD3.

4.5.9.6 Installing and Configuring Exchange Mail Server

The first task in the installation of Exchange Server 2019 in EXMB1 is to prepare the Active Directory environment where the Exchange Server will be placed, followed by the installation and configuration of the Prerequisites. And after that, installing an exchange will be the next step. The Exchange server 2019 has two roles: the mailbox role and the edge server role. The mailbox role is intended for storing mailbox databases, and the exchange edge server role is for routing email to clients.

The next step in the installation and configuration of exchange server 2019 is post installation configuration, like creating a new outbound and inbound send connector to send emails to internet email, Configure Virtual Directories, Configure Outlook Anywhere, Set Service Connection Point, Rename default database and move database path, Install Certificate.

Once exchange server 2019 is installed and configured in EXMB1, the next step will be doing the same thing in EXMB2 and then creating a Database Availability Group for the two mailbox servers DAG1 with member servers EXMB1 and EXMB2. The witness server will be the primary domain controller, ad1.local.com.et in this case.

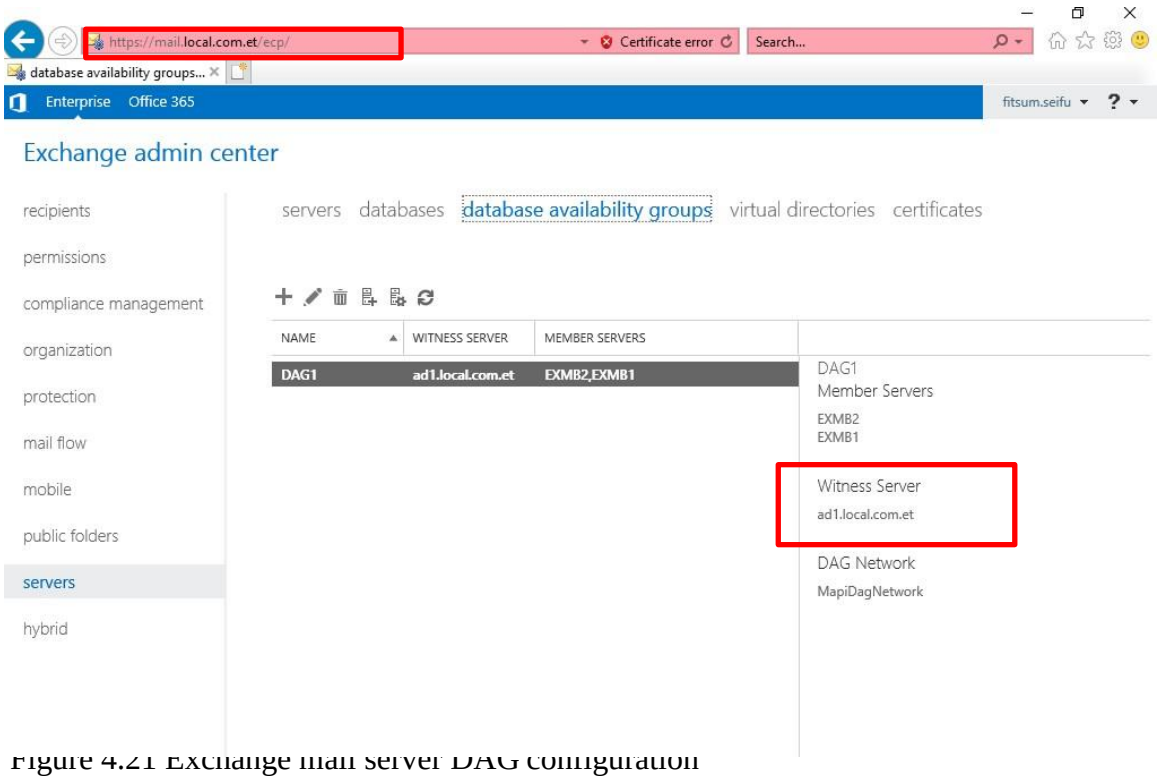

Figure 4.21 Exchange mail server DAG configuration

The next step will be enabling DNS round robin for load balancing purposes, and pointing the two mailbox servers to the same DNS A record, in this case, creating A record for the primary mailbox server EXMB1and secondary mailbox server EXMB2 on the active directory DNS server, and pointing it to mail.local.com.et as shown in Figure 4.22 and Figure 4.23.

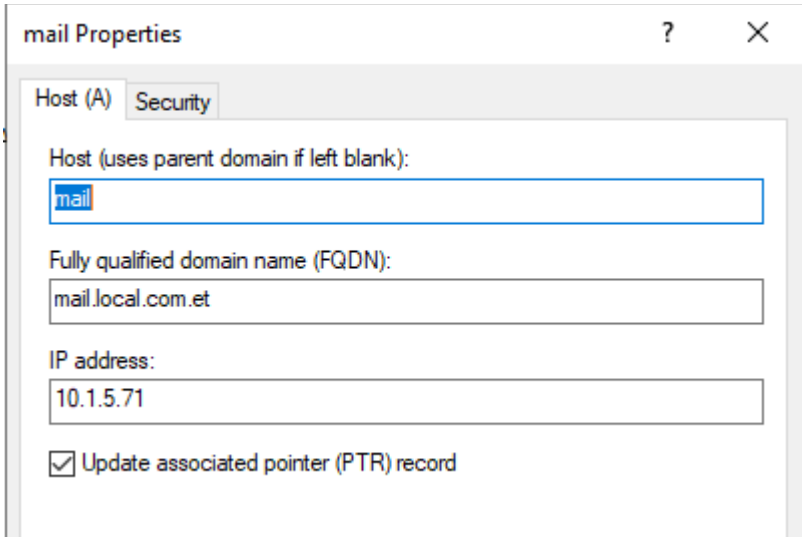

Figure 4.22 Host A record of Exchange Server EXMB1

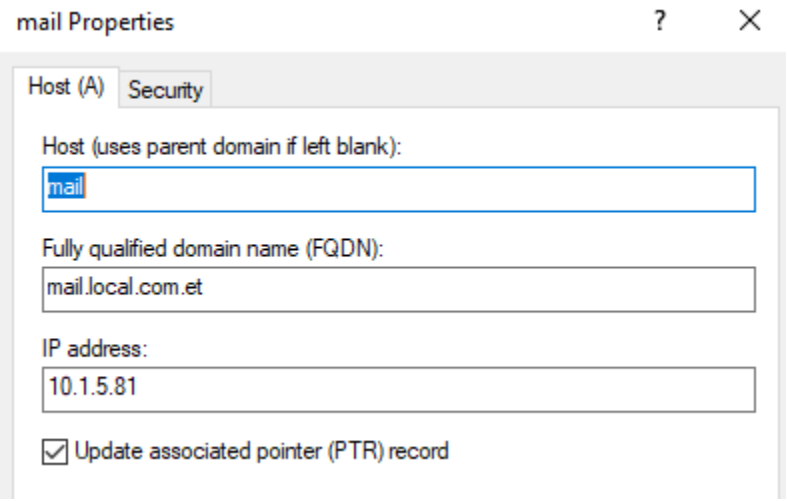

Figure 4.23 Host A record of Exchange Server EXMB2

After the two mailbox servers' IP addresses point to the same A record, mail.local.com.et, the DNS round robin configuration or load balancing configuration will forward mail traffic to one of the available mailbox servers according to the activity or the availability of the server.

Because the two servers point to the same A record, users will not know which mailbox server they are accessing their email from when they try to access their email via the web or other third-party mail access applications. Therefore, when users type https://mail.local.com.et in the address bar, the traffic will be redirected to the available server.

Next step will be checking whether mail replication between the two servers are working using a command, the command should be executed from exchange management shell command interface. Opening exchange management shell with administrative privilege, and type the command Test-Mailflow EXMB1 –TargetMailboxServer EXMB2 and press inter, as shown in Figure 4.24, the TestMailflowResult indicate success. Therefore, the replications between the two servers working properly.

```
[PS] C:\Windows\system32>Test-Mailflow EXMB1 -TargetMailboxServer EXMB2


RunspaceId          : d272f327-90e1-4d4d-8756-d8f28f8ebef1
TestMailflowResult  : Success
MessageLatencyTime  : 00:00:27.3529102
IsRemoteTest        : True
Identity            :
IsValid             : True
ObjectState         : New
```

Figure 4.24 Test mail flow between Exchange Server EXMB1 and EXMB2

The next step will be checking if individual mailbox address is working properly, using

exchange management shell with command:

Test-Mailflow –TargetEmailAddress fitsum.seifu@local.com.et, as shown in Figure 4.25, the TestMailflowResult indicate success.

```
[PS] C:\Windows\system32>Test-Mailflow -TargetEmailAddress fitsum.seifu@local.com.et


RunspaceId          : d272f327-90e1-4d4d-8756-d8f28f8ebef1
TestMailflowResult  : Success
MessageLatencyTime  : 00:00:02.8042356
IsRemoteTest        : True
Identity            :
IsValid             : True
ObjectState         : New
```

Figure 4.25 Test mail flow between Exchange Server EXMB1 and mail address

Now let's shutdown primary mailbox server EXMB1 and try to access email address of fitsum.seifu@local.com.et.

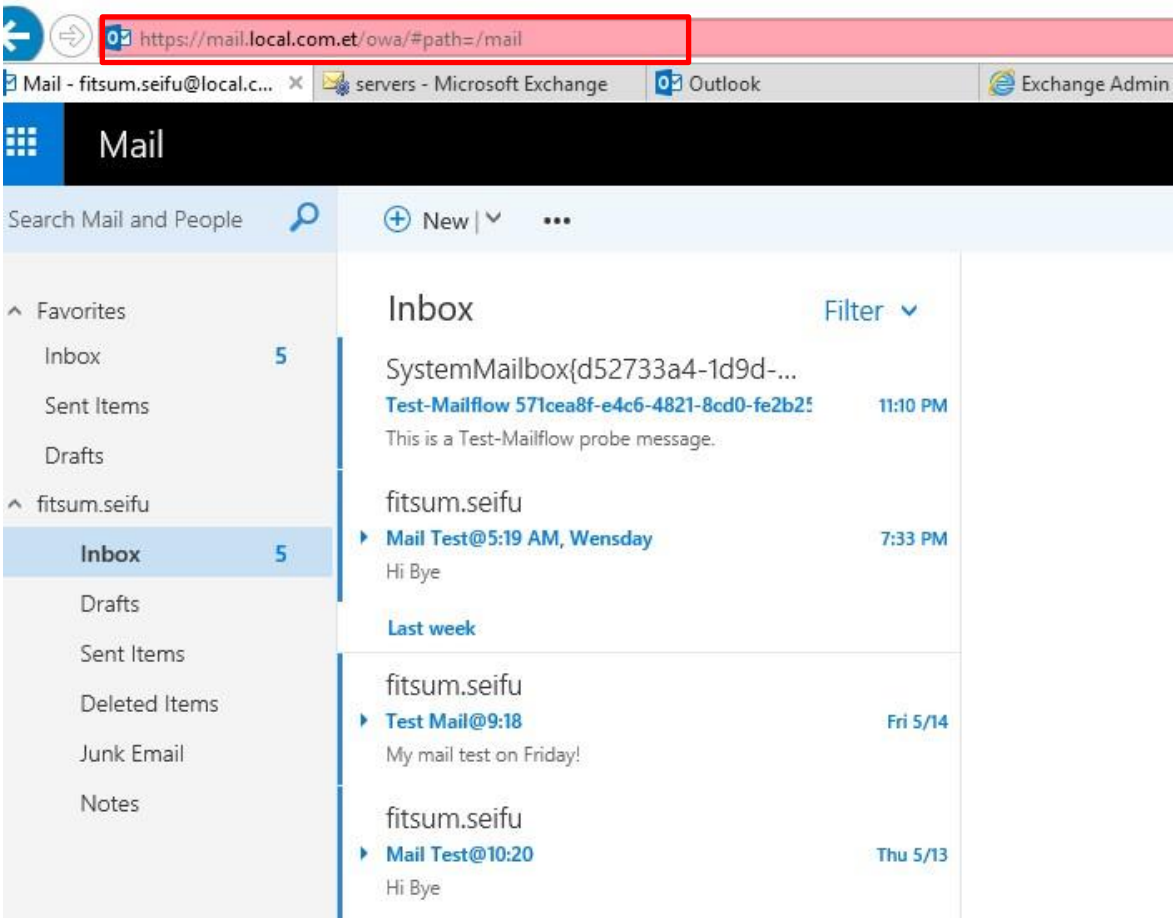

Figure 4.26 Test mail access of individual email address

From the results, we can conclude that, if one of the mailbox servers is down for different reasons,

like system maintenance or system crush, users are still able to access their email because email content is replicated within each mailbox server database using a DAG configuration as shown in Figure4.26. And when the user tries to access using web interface or other client mail access tools, in this case using web browser simply: https://mail.local.com.et/owa, the traffic will be redirected to one of the available server, and the user can access email without noticing from which mailbox server they are accessing.

4.5.9.7 Installing and Configuring Trading Application Servers

To create accessibility of trading applications, primary active directory servers configured on the DR site should be available because all the trading applications highly depend on active directory servers. Considering resource planning for trading application configuration, the exact copy of the configuration of all trading servers should be available on the DR site.

Since real-time data access for trading applications is mandatory, therefore, the availability of a database server on the DR site should be a must and the data present in the database has to be real-time data. This issue will be addressed by the proposed database architecture implementation on the DR site.

Hence, all trading applications are published on IIS 6. To create a high-availability disaster recovery of applications from the DR site, this study proposes failover clustering for high availability & load balancing between servers and DFS replication for replication of source code data between the two servers. This method is implemented in two steps: first, we create two servers with identical hardware and software specifications, and then we create failover clustering for high availability of the two application servers.

During the first step of this implementation, the failover clustering feature is installed on the two application servers, and configured for failover clustering prerequisites, such as configuring two network interface cards for each server, one for communication and the other for replication, as shown in Figure 4.27.

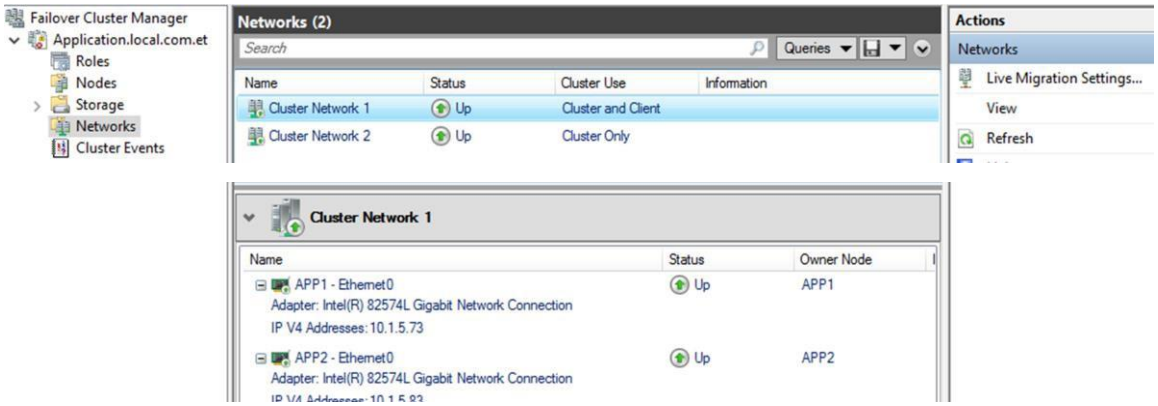

Figure 4.27 failover configuration of two servers network configuration

The next step will be adding the two servers to the failover group, Application.local.com.et in the Node part of the configuration, as shown in the Figure4.28.

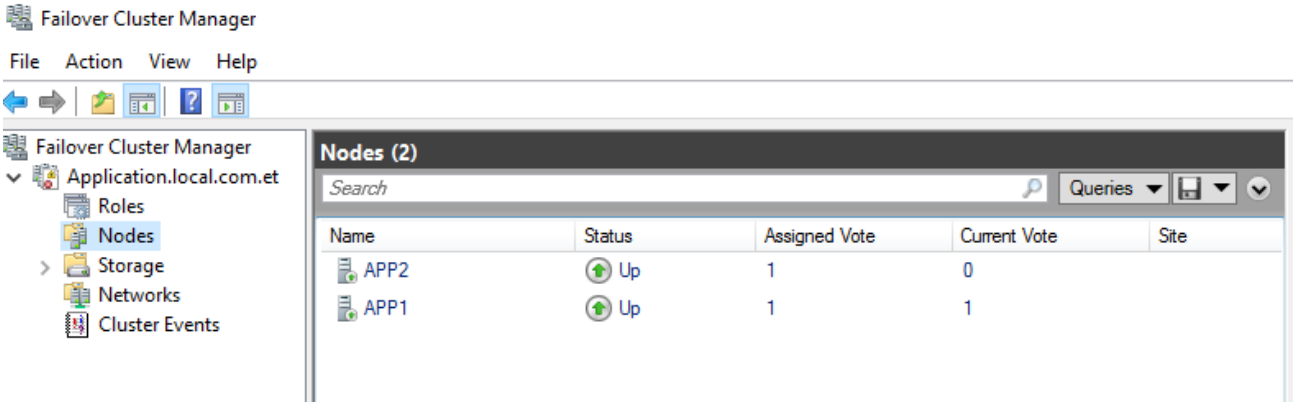

Figure 4.28 failover configuration of two servers APP1 and APP2

Following the creation of cluster group membership, the next step will be to create a DNS A record for the two servers, which in this case an application named sacco and published in IIS. Therefore, the A record of the two servers points to sacco.local.com.et. So when the user opens the sacco application using a browser, http://sacco.local.com.et, the failover clustering feature will forward to one of the available servers and the user will not notice which server is up and running.

The second step of this configuration is publishing the source code of the two servers in IIS, having the same replication directory. In both cases, the E:\DATA directory is created and the source code is placed here. The first step in this process is installing the DFS namespace and DFS replication for application servers APP1 and APP2. A Distributed File System (DFS) is used to organize distributed SMB file shares into a DFS Server. The distributed file system is used to replicate files and folders on multiple servers. In this implementation, the source code will be replicated.

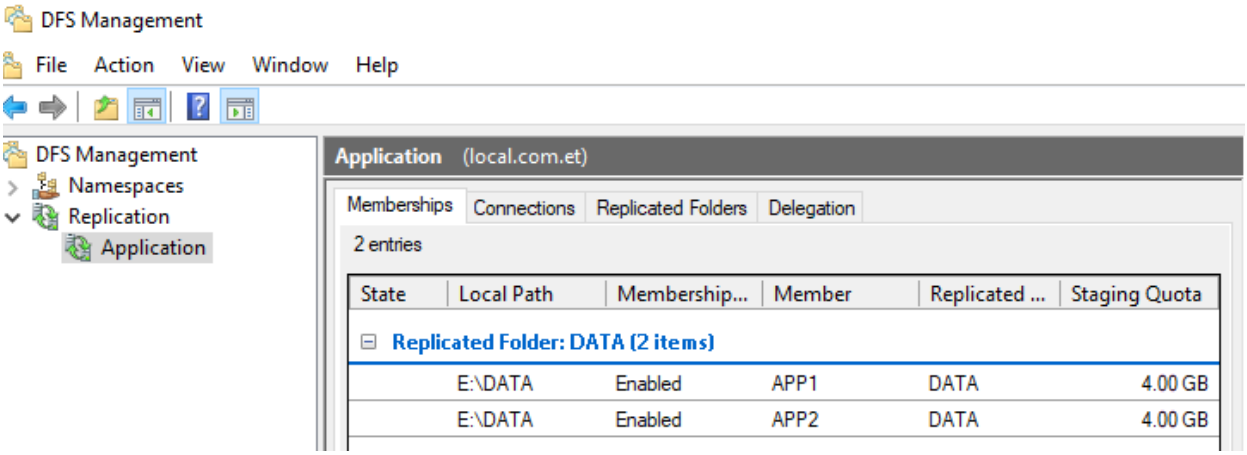

Figure 4.29 DFS replication configuration of two servers APP1 and APP2

During DFS configuration, the first task will be creating a DFS replication group, then adding member servers to the replication group, then selecting the replication topology, after selecting the topology specifying the replication schedule and bandwidth. In this case, continuous replication is selected. In both cases, the next step will be to select the replication directory, E: \ DATA. The last step of this configuration is testing the replication with some text files.

The final step in both configurations is to test the availability of the application servers. To begin, assume that the primary application server is unavailable due to maintenance or system crushing. In this case, let's shut down the application server APP1. As shown in Figure 4.30, APP1's status is down, and the current vote has changed to 0, indicating that it's unavailable.

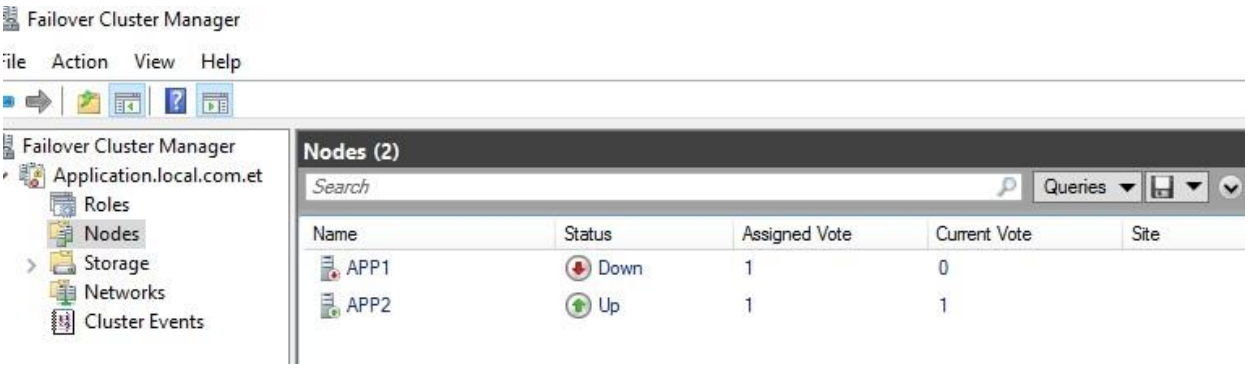

Figure 4.30 failover configuration of two servers APP1 and APP2

Now let's try to access the application sacco using browser internet explorer, http://sacco.local.com.et.

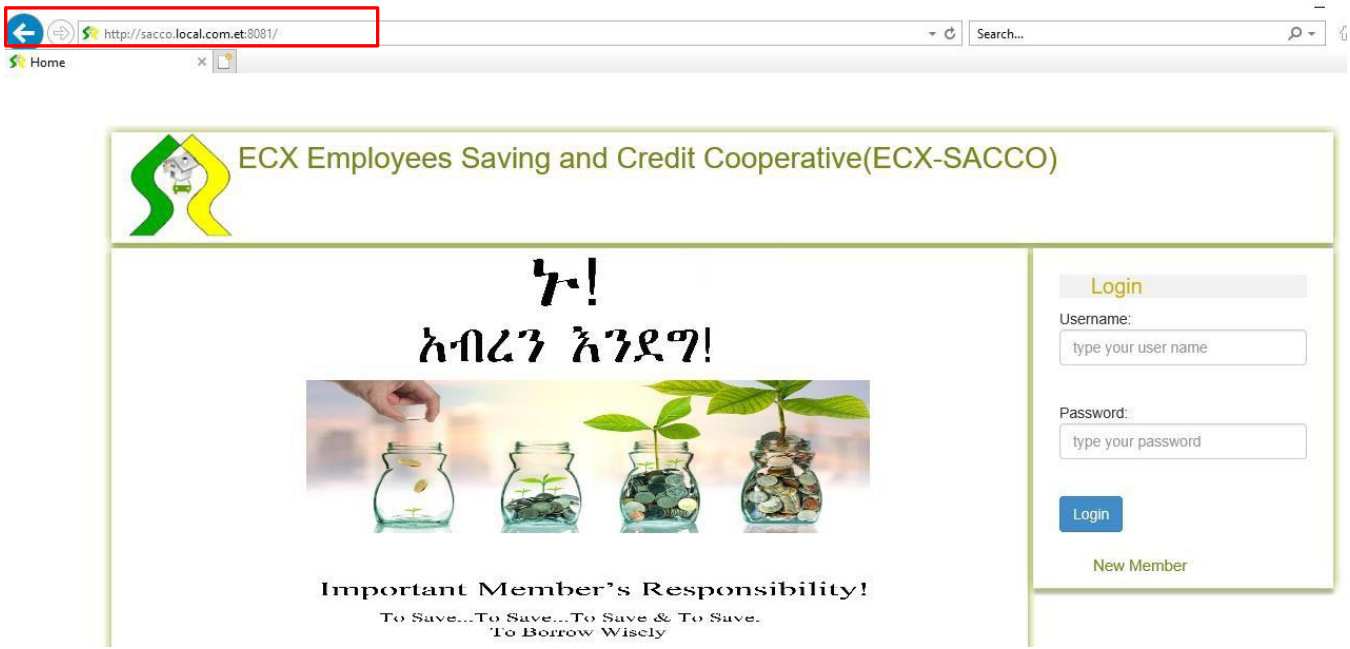

Figure 4.31 application access of two servers APP1 and APP2

From the results obtained, even if the application server APP1 is down, it's possible to access the application. Therefore, whenever one of the application servers is down, users are still able to access the application, in this case, the sample application Sacco, using http://sacco.local.com.et:8081.

The node accepting the traffic is determined by the vote priority setting of the cluster nodes. As a result, whenever trading servers are unavailable, the user's request traffic is redirected to the next available server.

4.5.9.8 Installing and Configuring Production Database Servers

Because database applications are critical to every business application, it is critical to implement database high availability. This study considers the database high availability configuration of database mirroring with a witness server configuration. Database mirroring provides database redundancy by transferring data from the transaction log to another instance of SQL Server. When it is necessary to have an automatic failover for a database, this is a good option. Depending on all of the options used, it can be a near-real-time database failover.

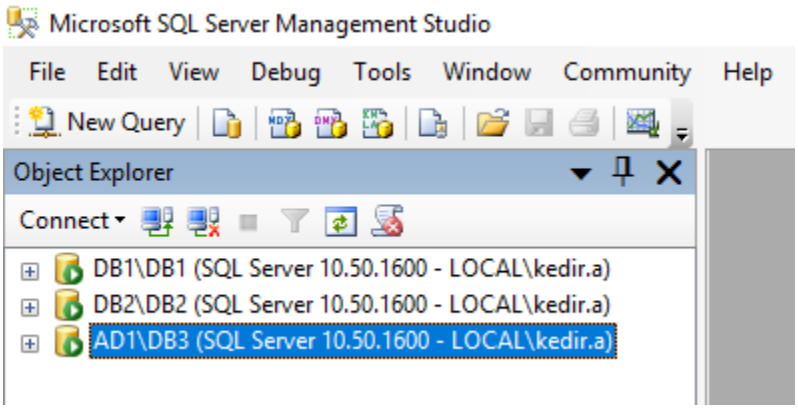

Figure 4.32 Database configuration of three servers

As shown in Figure 4.32, there are three database installed servers of which DB1 is the primary database server and DB2 is the mirror database server. In this study, the active directory server AD1 is used as a witness server because the active directory server is responsible for every authentication of users.

Failover clustering, which provides high-availability support for an entire instance of SQL Server, is another method for ensuring database availability. A failover cluster is a combination of one or more nodes, or servers, with two or more shared disks. This method has the problem of a single point of failure. The shared disk is where all the database configuration information and data is stored. Therefore, if the disk is unavailable or down for some time, a total outage of the system will occur and this study doesn't recommend this method.

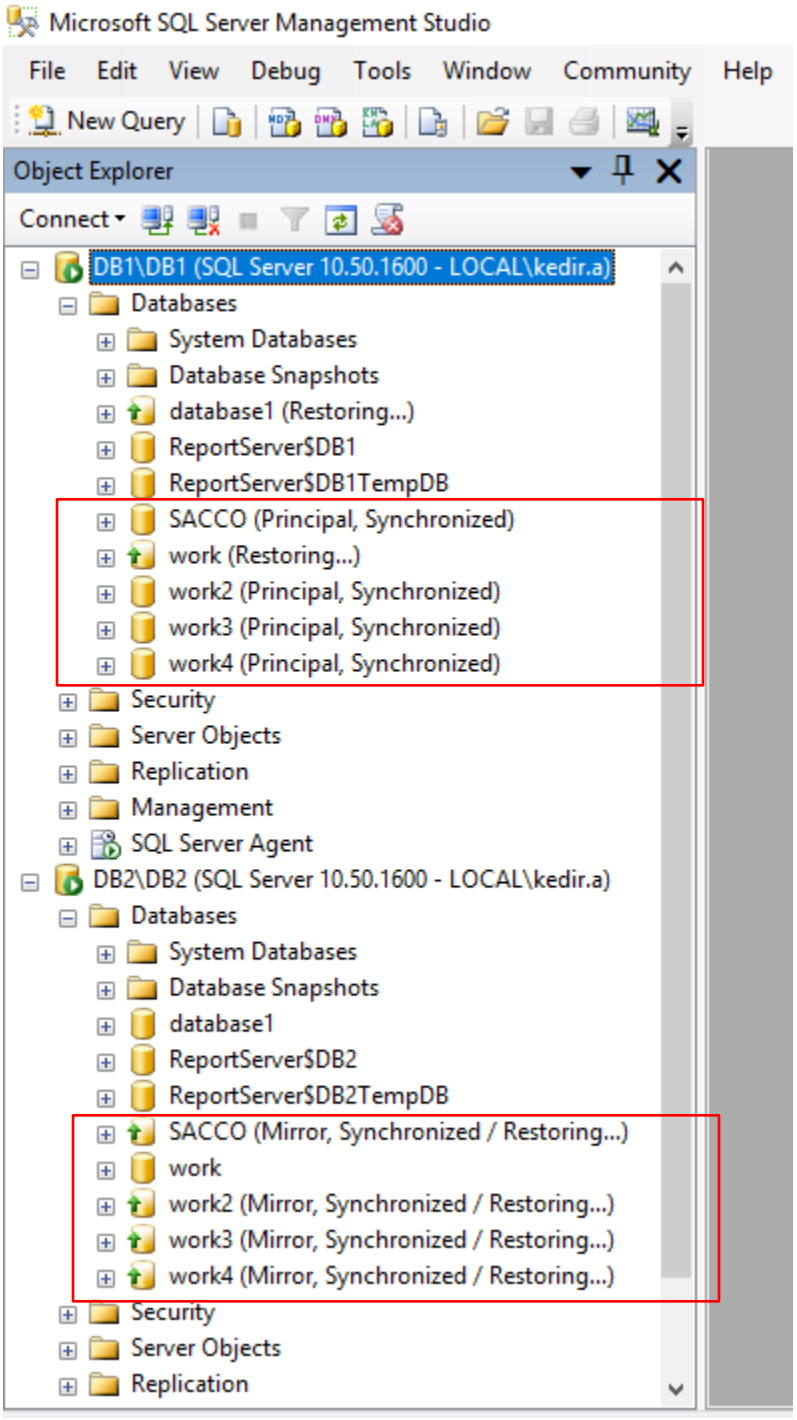

Figure 4.33 Database configuration of DB1 and DB2

The DB1 server is the primary database server, and the DB2 server is the mirror database server, as shown in Figure 4.33. In database mirroring, the primary database server is a read-write database that has its transaction log entries applied to a read-only replica of the database (a mirror database). A mirror database is a duplicate of the primary database that is normally fully synced with it.

This implementation technique employs automatic failover, which involves the mirror server

taking over the role of the principal server and bringing its copy of the database online as the principal database when the principal server becomes unavailable. AD1 was used as a witness in this case.

Now let's start to test if DB1 is shut down and DB2 is up and running, as shown in Figure 4.34, DB1is red means that, it's down & disconnected and refreshing DB2, makes it principal server.

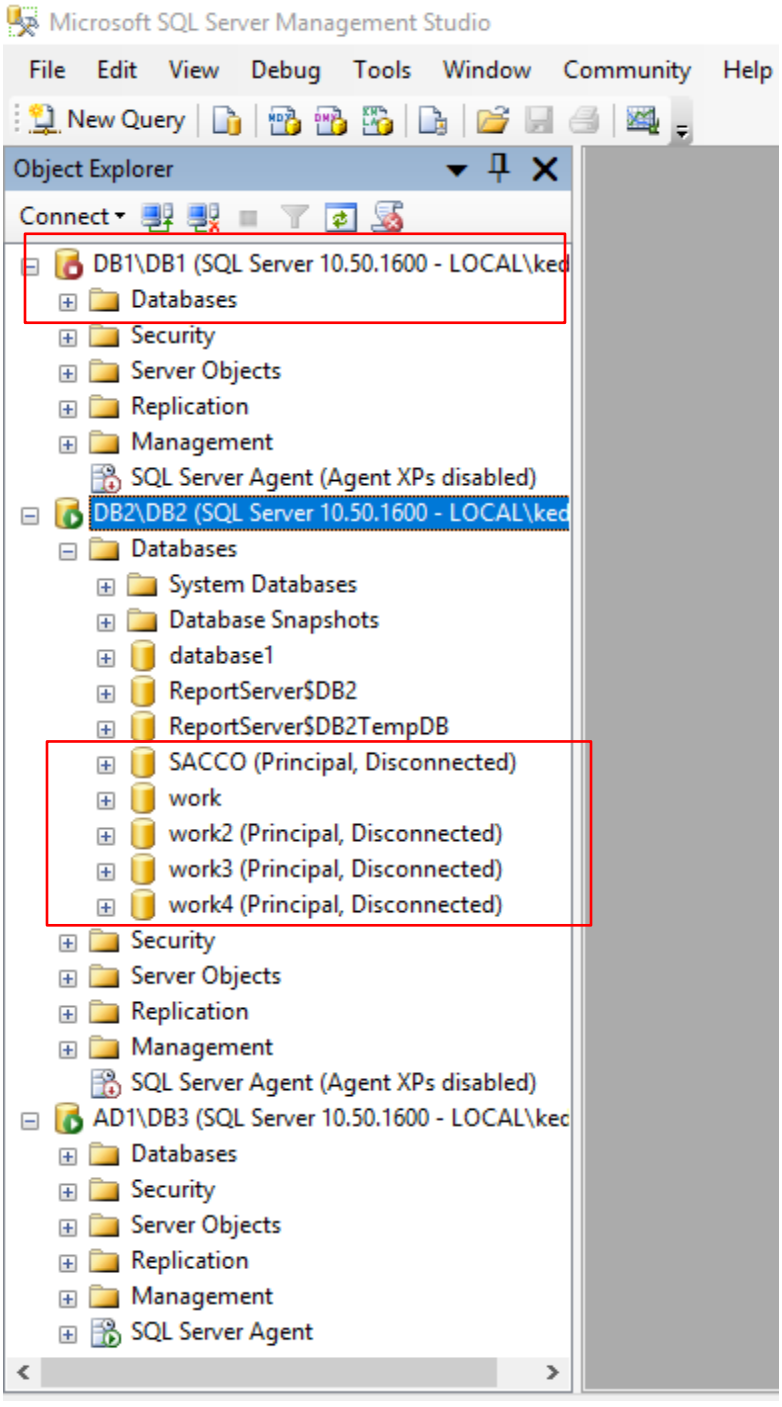

Figure 4.34 Database configurations of DB1 and DB2 with DB1 down

From the results obtained, if one of DB server is down, the witness server detects and automatically failover to working database server. As a result, this configuration creates high availability of database systems and users will not be able to know from which DB server they are accessing the data.

4.5.9.10 Chapter Summary

This chapter presented data analysis, representation and implementation. The study began with a review of data analysis procedures and then narrating interview questions replies, and providing a visual diagram of the data. Review of different industry standard architectural designs and design existing architectural design of critical business applications including trading applications.

Then came the implementation methods, which were divided into phases: Phase 1: Identifying and Analyzing Resource Requirements, Phase 2: High-Level Design of Existing Architecture to Demonstrate What's Needed, Phase 3: Proposed Architecture High-Level Design, Phase 4: Implementation of Proposed Architecture, which includes a study of the Production Site, capacity planning for the Production Site, capacity planning for the Disaster Recovery Site, and experimental setup and tests of the proposed architecture.

Chapter Five

5. Discussion, Conclusion and Recommendation

5.1 Introduction

The presentation and analysis of data was covered in the previous chapter. Chapter Five consists of a summary of the study, discussion of the findings, limitations of the study, recommendations for further research, and conclusions. The purpose of the latter sections is to expand upon the concepts that were studied in an effort to provide a further understanding of the implementation of high-availability disaster recovery with active/standby implementation. Finally, a synthesizing statement is offered to capture the substance and scope of what has been presented in this research.

5.2 Major findings of the research

The goal of this study was to find a gap in disaster recovery strategy execution during the use of information technology resources in Ethiopia's commodity exchange's day-to-day operations.

The study takes a qualitative approach, with data collected through structured interview questions and a case study to determine the organization's main business.

To understand basic concepts, a detailed literature review was conducted, and references to various industry standard architectural frameworks such as Microsoft, Dell, IBM, Sisco, Oracle, Linux, and others were taken into account when designing the architecture of existing business critical applications and when developing new ones.

Because it is necessary to obtain input from multiple subject matter experts during the duration of the project, and it’s known that, the success or failure of the project is strongly dependent on the project team. Therefore, there should be a mechanism to work with people from all major sectors of the firm in order for the project plan to be successful. The types of teams needed are determined by the system in question. The size of each team, team names, and organizational hierarchy are all determined by the organization.

During the study, it was identified that there are policies and procedures to identify risks related to IT infrastructure, IT Security, Application Development, and network systems. Once the risks are identified, they will start to develop mitigation strategies in discussion with IT Divisions. However, it has been determined that there is no proper method of identifying risks related to business critical applications. However, during the interview, the security team revealed that there are various risks

identified, such as unauthorized access, scalability issues with different platforms, misuse of business critical applications, full or partial business interruption, data loss, etc, have been identified.

Scholars suggest that, to successfully determine the specific risks to an IT system during service interruption, a risk assessment of the IT system environment is required. In a reply from the Application Development Manager, until now, they didn't perform risk assessment of business critical applications, and also, they didn't perform business impact analysis. Scholars have agreed that proper risk assessment will be used as an input to business impact analysis. As a result, at this stage, core business units and core business applications will be identified, as well as the interdependency of mission critical business applications identified.

The study identified that backups of databases and mission critical application backups are taken as an offsite backup. And the type of disaster recovery site is a cold disaster recovery site, and the link speed is slow. Therefore, replication of data between sites will be difficult.

Using a backup is one means of restoring a business from a significant disruption, and the typical reason for taking backups and/or archiving is for future use, with the length being short or long. This study identified that, there are trends of taking a backup of mission critical applications within the organization. And the frequency of taking backup of mission critical applications such as windows system state, exchange mail is daily, for Database backup every hour, and application backup on weekly basic or when there is a change. Considering the order of recovery for business critical applications they use different parameters such as criticality, relevance, sequence etc. they give high priority for critical applications such as active directory, database system, trading, clearing and settlement, central depository, surveillance and membership applications to be recovered immediately.

More comprehensibly testing the plan, it checks for understanding of the processes, procedures, and steps defined. It validates the integration and dependencies of tasks across various business and functional units. But without having a proper disaster recovery plan, it's difficult to discuss testing of a recovery plan, like suggested earlier there is no disaster recovery plan in the organization.

5.3 Discussion

This thesis has explored how designing an architectural framework for critical business applications with the best practice of different industry standards helps to improve resource management, simplify deployment, and increase the resilience of modern business critical

applications with their implementation strategies. This study proposed a set of automated, application generic techniques that exploit the speed and flexibility of recovery strategy to handle the scale and dynamics of applications.

Research question one: What are the key business processes and dependencies that exist between each process? Which business processes require high availability during operation?

This study identified that there are key business processes such as trading operations, clearing & settlement service, warehouse service, central depository, and other routine business operations of sales, payroll processing, customer relationship management, office communication, and employee data processing. There are various business-critical applications for each business process.

Trading platforms, which bring buyers and sellers together to exchange commodities, as well as trading operations applications, are critical to the business process. Therefore, there should be a way to make it available for trading applications. During the interview for data collection, key business critical applications are identified, and the dependencies between each business critical application are identified and documented in Table 4.1 of this document.

For each business critical business application, the dependency that exists in between them clearly defines which role must be present for the proper functioning of those business critical applications. For example, for a trading application to function properly, its components must function properly, the database system must contain up to data with no data inconsistency, and the active directory service must be available for proper user authentication and access control. With this, therefore, the dependency mapping of each business critical application should be kept for proper functioning of each application and overall IT infrastructure system required to work properly.

Research question two: How would the business function in a backup recovery site? What would be needed in terms of staff, equipment, supplies, communications, processes, and procedures?

Disaster recovery is like an IT project management system. One of the basic steps is creating a disaster recovery project team and the project's success or failure highly depends on the project team because it’s mandatory to get input from various subject matter experts during the course of the project. The study identified that, currently there is no disaster recovery plan, policy and procedure. As a result, resuming normal business operations is extremely difficult.

Currently, when a business disruption occurs, a team will be formed based on hands-on experience in the industry and knowledge of the business process. For the project plan to be successful, it must work with people from all key areas of the company. System administration, network,

database, application, and storage administration skills are required, according to the study. And a key role should be played by system and storage administrators.

The study reach into a solutions of how to recover each business critical applications based on developed architecture. Before start to implement disaster recovery of each business critical application, the study developed a recovery strategy and next step will be implementation and the implementation detail is specified in the Implementation method part of this document.

5.4 Conclusions

During the course of this study, it was identified that most previous studies mainly focused on the status of implementation of disaster recovery planning in the banking industry. However, this study focused on developing the architectural framework of business critical applications and then proposing implementation strategies for high-availability and disaster recovery site.

This study used disaster recovery planning phases to develop interview questions for data collection, and valuable outputs were identified in each phase: in the project initiation phase, the study attempted to identify how disaster recovery planning was initiated; in the risk analysis phase, the study identified critical business risks; and in the business impact analysis phase, the study used the risk assessment as an input and identify critical business applications, their dependencies and recovery priorities of those critical business applications.

Inventory is the next step in disaster recovery planning, and it focuses on the hardware and software inventory of IT resources. The study is currently attempting to identify resources and map existing business critical applications in order to determine what is necessary for the proposed system. The recovery plan is the next step. The study determined what should be included in the recovery plan and how it will be implemented at this point. The recovery strategy stage comes after the recovery planning step and develops a recovery strategy for essential business applications.

Following all of these steps, the study developed implementation strategies for a high-availability disaster recovery site, which were divided into different phases: the first phase tries to address Analyzing and Identifying Resource Requirements, the second phase develops High Level Design of Existing Architecture, to show what is required, and the third phase develops High Level Design of the Proper Architecture. Through different steps, such as study of the Production Site, Capacity Planning for the Production Site and Disaster Recovery Site, and finally, experimental

setup and tests of the proposed architecture are performed.

After identifying each business critical application, a recovery strategy for each application is developed. During the study, it was identified that the active directory is the main critical application, and each business critical application highly depends on it. And to create high availability, this study suggests active directory replication between primary and disaster recovery sites, having a primary and secondary configuration at each site.

Next to active directory, the study identified that the database application is the other main critical application and suggests that database mirroring with witness server implementation method used. Data is replicated between primary site and DR site and the witness server helps to detect which site database system is unavailable.

It is identified that, every trading applications are running in a web-based environment and their dependencies are identified and documented in this document. These trading applications highly depend on the proper functioning of the active directory and the database system. This study recommends failover clustering with the DFS replication method to achieve high availability of trading applications. Failover clustering balances application request traffic between available servers, and DFS replication aids in source code replication between each member server.

The other business critical application that should be highly available is exchange mail service, and to create high availability of mail service, this study suggests the same capacity mailbox and edge server implementation in primary and DR sites and a DNS round robin for load balancing traffic between available servers.

Finally, to conclude, for each high availability implementation strategy of critical business applications, the best practices of each implementation method are considered and recommendations from subject experts are advised.

5.5 Limitations of the study

The primary focus of this research was identifying the gap in the implementation of high-availability disaster recovery sites using an active/standby implementation architecture. During data collection of this study, few staff, because of their huge responsibility in the organization, it was difficult to get them.

Different organizations have different business processes, and critical business processes in one organization may not be critical in another organization and also the dependency of each process may be different. More importantly, they may have different IT platforms, such as Windows or

Linux. As a result, the recovery strategy will be different. Therefore, the findings of this study may not be applicable to other financial sector organizations or banks.

During implementation and Evaluation of this study, it was difficult to get required IT infrastructure including Virtualized Servers, Storage space and required software. As a result, the study forced to consider minimum requirement of Hardware resource for the implementation of business critical applications.

5.6 Recommendations

There are no disaster recovery plans in place for all of the organization's systems that serve critical business functions. Furthermore, none of the organization's disaster recovery processes have been found to be robust enough to recover all critical systems effectively and efficiently in the case of a disruption.

As a result, the following points are suggested by this research:

- The organization should have a proper disaster recovery plan in place, as well as a disaster recovery team with the necessary educational qualifications and business process experience.
- Create a disaster recovery team made up of members from all major departments of the organization, with the necessary team size and titles.
- The business must give sufficient training to employees with specialized disaster recovery roles and duties in order to provide them with the knowledge and skills necessary to manage a system's recovery after a disruption.
- Develop a disaster recovery testing, which helps the organization to verify their ability to recover IT systems after a major disruption. A disaster recovery test involves recovering and restoring an IT system by following the procedures defined in a disaster recovery plan.
- The Business Impact Analysis (BIA) phase refers to the process of identifying an organization's Critical Business Functions, and the organization shall perform a scheduled BIA as a result, helps to identify critical business processes, the dependencies that exist within critical business processes, and helps to prioritize business process and s recovery.

Further recommendation from this study is listed as follows:

- Risk assessment team should be established.
- Perform Asset inventory of hardware and software for the IT infrastructure.
- Identifying the resource mapping matrix for newly configured hardware and software of Servers.

- RTO and RPO of mission critical application should be identified.
- Backup policy and procedure should be prepared.
- Backup technology should be selected, and backup media should be prepared.
- Disaster recovery site should be prepared based on international standards.
- Disaster recovery site replication from primary site with proper replication strategy should be selected.
- Order of recovery for business critical application should be prepared and implementation strategy should be developed.
- During business disruptions what is needed in terms of staff, skills required, procedures and communication should be prepared and documented.
- Contract with vendors (SLA), software license, system user manuals, security manuals, and operating procedures should be documented.
- Disaster recovery policy and procedure document should be updated and distributed to concerned departments accordingly.
- The business recovery strategies should be developed, specific backup and recovery organized, policies and procedures should be developed and tested first.
- Once the BC/DR plan is developed, it's mandatory to implement methods for managing change through change management system.

5.7 Future works of the study

The main purpose of this study is to identify the gap in the implementation of a high available disaster recovery site and design architectural framework, findings are based on the data gathered during interview from subject experts, and the key findings of this study may not be applicable to other financial business sectors. Therefore, researchers can further investigate in the following areas:-

- Best practice in the implementation of Disaster Recovery Planning in manufacturing industries.
- Disaster recovery planning implementation methods for critical and non-critical business processes.
- Investigating the status of disaster recovery planning practice in non-financial sectors.
- Preparation and Testing of Disaster recovery planning document for Government offices.

References

[1] Cathy Baird (2003), Oracle High Availability Architecture and Best Practices, 10g Release 1 (10.1) Part No. B10726-01

[2] IBM, 2016, High availability overview 7.1, IBM i 7.1 (product number 5770-SS1),

[3] Susan Snedaker (2007), Business Continuity & Disaster Recovery for IT Professionals

[4] Vyshnavi Devi Jorrigala (2018), Business Continuity and Disaster Recovery Plan for Information Security

[5] Leonidas G. Anthopoulosa, Efrosini Kostavarab, John-Paris Pantouvakisc (2012), An Effective Disaster Recovery Model for Construction Projects, 26th IPMA World Congress, Crete, Greece, 2012.

[6] Haylay Gerezgiher (2017), an investigation of current status of IT disaster recovery plan in Ethiopian Banking Sector.

[7] Nigussie Birhanu (2017), Assessment of IT disaster recovery practices in Ethiopian commercial banks.

[8] Nigussie Tariku & Lemma Lessa (2020). Information Technology Disaster Recovery Plan (ITDRP) Framework for Banks in Ethiopia.

[9] Logan Vadivelu , Eduardo Patrocinio (2020), IBM, Distinguished Engineer, High availability and disaster recovery for your on-premises app. Retrived From:

https://www.ibm.com/garage/method/practices/manage/hadr-on-premises-app/

[10] Samson O. Chukwuedo (2015), Building theoretical and conceptual framework for qualitative research report in education, African Journal of Studies in Education, Vol. 10, No. 2, 2015. Pp. 83-101

[11] Ewnetu H. Tamene (2016), Theorizing Conceptual Framework, Asian Journal of Educational Research, Vol. 4, No. 2, 2016 ISSN 2311-6080

[12] Aileen Cater-Steel and Latif Al-Hakim (2009), Information systems research methods, epistemology, and applications

[13] Alan Hevner · Samir Chatterjee (2010), Design Research in Information Systems Theory and Practice

[14] Divya Krishnamoorthy (2012), Disaster Recovery Planning, NASA IV & V ANNUAL WORKSHOP, the 4th International Workshop on Independent Verification & Validation of Software.

[15] John W Creswell (2007), Second Edition QUALITATIVE INQUIRY& RESEARCH DESIGN Choosing Among Five Approaches.

[16] Marguerite G. Lodico, Dean T. Spaulding, Katherine H. Voegtle (2006) METHODS IN EDUCATIONAL RESEARCH from Theory to Practice.

[17] Vijay Vaishnavi, Bill Kuechler, Stacie Petter (2004), DESIGN SCIENCE RESEARCH IN INFORMATION SYSTEMS [Overview of Design Science Research] [Design Science Research Methodology] [Philosophical Grounding of Design Science Research] [Outputs of Design Science Research] [An Exemplar of IS Design Science Research] [Design Science Research Bibliography]

[18] Terry Critchley (2015), High Availability IT Services, International Standard Book Number-13: 978-1-4822-5591-1

[19] Joseph Sack, Sanjay Mishra (2012), SQL Server Technical Article, Always On Architecture Guide: Building a High Availability and Disaster Recovery Solution by Using Always On Availability Groups.

[20] Tonette S Rocco, Maria S. Plakhotnik (2009), Literature Reviews, Conceptual Frameworks, and Theoretical Frameworks: Terms, Functions, and Distinctions.

[21] Emad Kamil Hussein, Dickson Adom (2018), Theoretical and Conceptual framework: Mandatory Ingredients of a quality research.

[22] A B M Moniruzzaman, Md. Waliullah, Md. Sadekur Rahman (2014), A High Availability Clusters Model Combined with Load Balancing and Shared Storage Technologies for Web

Servers, International Journal of Scientific & Engineering Research, Volume 5, Issue 12, ISSN 2229-5518

[23] Mitch Tulloch, (2014) Training Guide Installing and Configuring Windows Server 2012 R2 Microsoft Press a Division of Microsoft Corporation.

[24] David Elfassy (2014), Mastering Exchange Server 2013 by John Wiley & Sons, Inc., Indianapolis, Indiana

[25] Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes (2010), Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34

[26] Dennis N. Hart and Shirley D. Gregor (2005), Information Systems Foundations: Constructing and Criticising.

[27] Christopher Kadlec, and Jordan Shropshire (2010), Best Practices in IT Disaster Recovery Planning Among US Banks

[28] Murizah Kassim , Maznifah Mohd Sahalan , Nur Izura Uzir (2018), Framework Architecture on High Data Availability Server Virtualization for Disaster Recovery

[29] Charlotte Brooks, Clem Leung, Aslam Mirza, Curtis Neal, Yin Lei Qiu, John Sing, Francis TH Wong, Ian R Wright (2007), IBM System Storage Business Continuity: Part 1 Planning Guide

[30] Aliisa Partio (2017), Data center Disaster Recovery & Major Incident Management

[31] Mohammad M. Al-shammari, Ali A. Alwan (2017), A Conceptual Framework for Disaster Recovery and Business Continuity of Database Services in MultiCloud.

[32] Timothy Wood, Emmanuel Cecchet, K.K. Ramakrishnan, Prashant Shenoy, Jacobus van der Merwe, and Arun Venkataramani (2010), Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges.

[33] Mueen Uddin, Sandun Hapugoda, Roop Chand Hindu (2015), Disaster Recovery Framework for Commercial Banks in Sri Lanka Article in Journal of ICT Research and Applications.

[34] David Nicol (2017), the Business Continuity and Disaster Recovery Framework and Policy

[35] VICTORIAN GOVERNMENT PRINTER (2017), ICT Disaster Recovery Planning, PP No

262, Session 2014–17

[36] Goh Moh Heng (2015), Business Continuity Management Planning Methodology, International Journal of Disaster Recovery and Business Continuity Vol.6 (2015), pp.9-16.

[37] Heather McCall Brotherton (2011), Data center recovery best practices: Before, during, and after disaster recovery execution.

[38] José G Vargas-Hernández, Osmar Arandia, Arturo Cordova-Rangel (2016), A Review of Research Methods in Strategic Management; What Have Been Done, and what is Still Missing

[39] Eman Al-Harbi Soha S. Zaghloul (2013), A SWOT analysis on Cisco High Availability

Virtualization Clusters Disaster Recovery.

[40] CR Kothari (1990), Research Methodology, Methods and Techniques, Second Edition

Appendix A: Interview Questions

Area	Questions	Answers
Project Initiation	1. How do you identify who will be working at the original site and who will be working at the alternate site?	
	2. What are the key skills, knowledge, or expertise needed to recover? What are the key roles that must be present for the business to operate?	
Risk Assessment	3. What are the natural and man-made disasters that could impact the business related to IT service?	
	4. What are the risks related to business critical applications?	
	5. What would happen if electricity to this site were cut or unavailable for half a day, one day, one week, one month?	
IT Inventory	6. What are mission critical business applications of your Department?	
	7. What information is documented for all mission critical applications?	
	8. What configuration information is documented related to mission critical applications?	
	9. How do you map resources to business critical applications?	
	10. What are the resources allocated for	

	each business critical applications?	
	11. How do you perform inventory of hardware and software related to business critical applications?	
Business Impact Analysis (RPO) indicates the amount of data (updated or created) that will be lost. **(RTO)** is the amount of downtime a business can tolerate.	12. For your Department mission critical applications, what are the maximum tolerable downtime (MTD), Recovery point objective (RPO), recovery time objective (RTO)?	
	13. What are the interdependency that exist between mission critical business applications?	
	14. What is the amount of data loss expected during a disaster?	
	15. How do you conduct business impact analysis for mission critical applications?	
	16. Which functional requirements for the business indicate what functions or abilities must be present in order to continue business operations after a major (or minor) business disruption?	
Recovery Strategy	17. What type of disaster recovery site do you have?	
	18. What type of off-site backup do you have, and for how long the backup retained?	
	19. How frequent do you take backup of mission critical applications?	
	20. What data replication strategy do you have between primary site and	

	alternate site?	
	21. What is the order of recovery for business critical applications?	
	22. What Critical Data Recovery Options you have? Data backup frequency, data backup type, data backup method?	
	23. How do you review mission-critical services to determine which applications should be restored first?	
	24. How would this business function in a backup recovery site? What would be needed in terms of staff, equipment, supplies, communications, processes, and procedures?	
Disaster Recovery Planning	25. What disaster recovery plan you have?	
	26. What are the policies and procedures you have for mission critical business applications?	
	27. How often do you review and updated the policies and procedures of IT disaster recovery?	
	28. How do you review internal and external data or application dependencies? Take action, as appropriate, to ensure all dependencies are addressed in the correct order and timing.	
	29. What recovery plan or procedure do you have to restore backup systems?	

Maintenance & Auditing	30. How Audit existing systems to ensure compliance with current BC/DR plans including: Operating systems, Networking and telecommunications equipment, Database and applications, Systems backups, Security controls, Integration and testing?	
Training & Testing	31. How do you review BC/DR plan to understand which mission-critical functions should begin, in what order tasks should be started, and what dependencies exist?	

Appendix B: Support Letter to ECX

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

Addis Ababa University
College of Natural Science
School of Information Science

Date: January 13, 2021
Ref No. SIS/08/2021/13

To Whom It Concern

Subject:- Student Fitsum Seifu W/Tensay

Dear Sir /Madam,

Student Fitsum Seifu W/Tensay (ID.No GSE/4652/11) is graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a M.Sc. Thesis research under the title "Designing a framework for implementation of High Available Disaster Recovery Site with Active-Standby implementation Architecture: Case of Ethiopia Commodity Exchange (ECX) ".

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

With Regards

Tibebe Beshah (PhD)
Head, School of Information Science

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