Global IME Bank

ग्लोबल आइएमई बैंक लि.

सबैका लागि बैंक

Information Technology Business Continuity and Disaster Recovery Plan

Revised: September 2020

सञ्चालक समितिको मिति २०७७-०६-०४ को
३६१ औं बैठकबाट स्वीकृत।

Preamble

In exercise to the power conferred by Section 22 of Bank and Financial Institution Act 2073 B.S and the Article of Association of Global IME Bank Limited, clause 5 (17) of the Directive No 6 of Unified Directive 2076 B.S of Nepal Rastra Bank, the Board of Directors of Global IME Bank Ltd has approved this guideline vide its ___ Board Meeting dated ______________ for implementation. The need of IT BCP & DRP Policy has been addressed in Nepal Rastra Bank Information Technology Guidelines 2012 and other directives and circulars issued by NRB. The guidelines require bank to have detail procedures and guidelines for prioritizing critical business functions, incident handling and how the institutions will manage and control identified risk.

Version Control

Version Control No.	Date	Remarks
Version 1	November 2017	Revised
Version 2	September 2020	Revised

Anil

Approval Sheet

[redacted]	Kimil Timilsina ISO	

[redacted]	Preeti Singh Manager- Strategy	Preeti Singh
	Anil Joshi Chief Information Technology Officer	Anil Joshi.
	Buddhi Akela Chief Risk Officer	

[redacted]	Mahesh Sharma Dhakal Sr. Dy. Chief Executive Officer	
	Ratna Raj Bajracharya Chief Executive Officer	

[redacted]	Board of Directors BOD No. 361 Date: 20th Sep 2020	

Table of Contents

Overview

The Business Continuity and Disaster Recovery plan for any organization require that organization to list all events in which it cannot continue normal operations and also list all contingency plans for such events. IT Department at Global IME Bank also has a Business Continuity and Disaster Recovery plan that list all events that disrupt Information Technology service delivery and also explain how IT Department plans to keep services operational during such events. The Business Continuity plan is vital for IT Department in Global IME Bank because services of the Bank are technology based and managed by IT Department. Since the services provided by IT are of technical in nature, IT Department focuses more on technical aspects than non-technical aspects that affect service delivery.

The need of BCP Policy has been addressed in Nepal Rastra Bank Information Technology Guidelines 2012. The guidelines require bank to have detail procedures and guidelines for prioritizing critical business functions, incident handling and how the institutions will manage and control identified risk. The BCP should include allocation of sufficient resources, allocating knowledgeable person etc. and should be reviewed periodically. The BCP related to natural and man-made disasters shall be as **Guidelines on Continuity of Business Plan** and **BCP with technical aspects** shall be as described in this policy.

Roles and Responsibilities:

- A senior official of bank shall be appointed as Head of IT Business Continuity Planning and he would be responsible for developing BCP, its regular updates, prioritization of critical business activities, recovery, testing, training and other aspects of BCP.
- A BCP team shall be formed and it should comprise of senior official from various departments as required and it should be formed in head office as well as in branch offices and align with guidelines on Continuity of Business Plan.
- IT Department shall develop Terms of Reference for summarizing of all services provided, lists all technical events which can disrupt these services, and provides details of plans to continue these services in event of various disruptions.

Factor Affecting Delivery of IT Services

There are various types of factors that can cause disruption of IT services. They can be categorized into non-technical factors and technical factors.

Non-Technical Factors

Non-Technical factors imply any factor outside the technical factors of IT services, which includes one or more of the following: natural disasters (example: earthquake, landslide, lightening, flooding, etc.), man-made disasters (example: war, terrorism, riot, blockage, chemical/biological warfare, etc.) to name a few. Whatever the cause, all these can impact smooth delivery of IT services.

Considering the scale of non-technical disaster(s), IT Department will take appropriate action to continue providing the services from the DC site itself. In event the services cannot be provided from NDC site, IT Department will take appropriate action to provide the services from DR site.

Technical Factors

Technical factors imply those factors that are attributed to hardware, software, or network level failure in a system. Hardware level failure can be attributed to failure in one or more hardware components of a system.

Software level failure can be attributed to failure of operating system software, application system failure, and/or database system failure. While hardware and software related failure can be specifically attributed to servers and/or other devices, the network level failure can be specifically attributed to breakage of data connectivity between two points causing disruption in service delivery. Network level failure may not directly impact functioning of server or other device, but it will disrupt service delivery.

Terms of Reference for summarizing of all services provided, lists all technical events which can disrupt these services, and provides details of plans to continue these services in event of various disruptions shall focus on following aspect.

COMMON TERMS

a. **Data Center (DC) Site:** The primary site from where the organization's services are provided.
b. **Nearby Data Centre (NDC Site):** The secondary site from where the organization 'services are provided, if there are issues on Data Center.
c. **Disaster Recovery (DR) Site:** The secondary site from where the organization's services are provided if there is a disaster of varying degree at the Data Center and Near Data Centre.
d. **Recovery Point Objective (RPO):** It refers to the point in time in the past to which data will be recovered.
e. **Recovery Time Objective (RTO):** It refers to the point in time in the future at which the service will be up and running regardless of where it originates at.
f. **Business Continuity:** It refers to the process of continuing business either through DC, NDC or DR with the focus being minimal RPO and RTO.
g. **Disaster Recovery:** It refers to the process of returning back to providing service from the original source.
h. **Service Level Agreement (SLA):** It refers to the agreement between the Bank and service provider of a respective service. The SLA shall remain in place till the lifetime of service itself.

COMMON PROCESSES

The following sequences of processes are to be followed for business continuity and disaster recovery process:

a. **Business Impact Analysis (BIA)** refers to the impact of disaster on the business and/or daily operations of the organization.
b. **Preventions Strategy** refers to the strategies used to minimize impact on daily business. The common processes for preventive strategy are as follows:
   - Hardware level SLA must be done for all servers and storage devices at DC, NDC or DR level.
   - Software level SLA must be done for all applications at DC or DR level.
   - Data backup of each system hosted at DC/NDC must be done either in real-time or in periodic basis on a separate hardware. However, the backup frequency must dictate by acceptable level of RT and/or by guidelines from the regulatory authority.

c. **Containment Strategy** refers to the strategies used to contain the impact of disaster on daily business and/or the impact on other services caused by this particular service.
d. **Business Continuity Strategy** refers to the strategies to continue the business to minimize impact on continuous operation and service delivery.
e. **Disaster Recovery Strategy** refers to the strategies the recover from disaster and return back service source it the original state.

Further, the following common steps are applicable for software applications services from central level, i.e. DC or DR level.

a. **Involvement of SLA vendor/service provider:**
   - **Against Hardware/Device Failure:** The hardware SLA vendor will be immediately called in for support to repair or replace the damaged hardware. The actual time of recovery will depend on the degree of damage caused to the hardware.
   - **Against Software Failure:** The application level SLA vendor will be immediately contacted or called-in for support based on the proximity of SLA vendor. Further, necessary coordination with the SLA vendor will be done to get the solution of software problem and the same will be implemented by following appropriate procedure.

b. **Recovery Strategy:** In case of a disaster, service can be provided from secondary source while the original source is in process of repair/restoration/replacement whichever is applicable. The original source can be repaired/restored/replaced and made available within the day time, i.e. when the Bank's branches are operational. Nevertheless, the Bank's IT Department will wait till off-hours to bring the original service source back in operation and discontinue service from the secondary source. This will be done in consideration of providing uninterrupted service during the daytime.

c. **Data Verification during Business Continuity and/or during Disaster Recovery Process:** Further, when providing service from secondary source and switching back to the main source, the Bank's IT Department will follow necessary procedure to verify data accuracy of respective services. Only if the data verification results are correct, then the data restoration to the secondary source or from secondary source back to the main source will be authorized. Data verification process is applicable for systems that require data restoration and differ according to each system.