NCC Bank

नेपाल क्रेडिट एण्ड कमर्स बैंक लि.

Nepal Credit & Commerce Bank Ltd.

Your Business Bank

Business Continuity
&
Disaster Management Framework
2018

Nepal Credit And Commerce Bank Ltd
Bagbazar, Kathmandu

Approved by:

687th Board Meeting

Held on 28th May 2018 (2075-02-14)

NCC Bank
नेपाल क्रेडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.
Your Business Bank

The Board Meeting No. 687th
held on 2075.02.14 (28th May, 2018)
has decided to approve, the

"Business Continuity & Disaster Management Framework, 2018"

Kapil Gnawali
Company secretary
2075-02-14

Table of Contents

Business Continuity & Disaster Management Framework, 2018

1. Overview

Banking business is basically inevitable public service that requires continuous, smooth and credible service delivery to the customers. Interruption of banking services gives an advertent effect on bank itself, financial sector and as a whole economy of the nation. Despite all the financial measures to ensure prudence of the business, measures for business continuity against such odds are equally indispensable. Past experience of devastating earthquake in different regions of the country, disturbances on various custom points due to political turmoil etc. are the best experiences to look upon.

Business Continuity & Disaster Management Framework (the Framework) is formulated containing the key information and procedures as the references that might be needed at the time of disaster recovery for business resumption, staff safety, system management, customer servicing and various other factors. The plans and procedures outlined in the framework shall be used in the situation of disaster where the Nepal Credit & Commerce Bank (the Bank) needs to resume the overall operations system.

2. Objectives

The objective of the framework is to form the formal structure for handling the time of crisis where bank suffers from the event of business continuity and disaster recovery. It addresses the key elements of safeguard employees' lives, protect customer and bank's assets, business and technology recoverability and Risk (both internal to the bank and external to the clients). These plans ensure clients prompt access to their funds and securities-related data during all Significant Business Disruptions (SBDs). "Significant disruption" refers to local or regional events that include short or long term disasters or other disruptions, such as natural disasters, fire, flood, earthquake, extended power interruptions, hazardous chemical spills, and other man-made disasters like acts of malice, and technical or infrastructure disruptions. SBDs can range in level from building-specific events (such as an isolated technology problem) all the way up to regional issues (a hurricane, floods etc. for examples).

It also incorporates the technological awareness and sensitivity analysis for keeping intact all kind of technological devices, services and networks. It includes procedures for all phases of disaster recovery and strategies. However, it can provide some guidance in the event of such a large scale disaster too. Failure to adequately manage these events, bank may not only losses, but also threatens their survival as business entities

A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.

The priorities in a disaster situation are to:

a) Ensure the safety of employees and visitors in the office buildings.

b) Mitigate threats or limit the damage that threats can cause.

c) Have advanced preparations to ensure that critical business functions can continue.

d) Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.

3. Assumptions

The viability of this framework is based on the following assumptions:

a) That a viable and tested IT Disaster Recovery Plan exists and will be put into operation to restore data center service at a backup site within five to seven days.

b) That the General Administration Department (GAD) has identified available spaces for relocation of departments/ branches which can be occupied and used normally within two to five days of a facilities emergency.

c) That the plans and procedures have been properly maintained and updated as required.

d) Regular awareness program conducted to the staffs and regular drilling conducted on IT related activities as the rehearsal for the unintended incident.

4. Functional Structure and Responsibilities

a. Business Continuity and Disaster Management Committee

A Business Continuity and Disaster Management Committee (to be called as "BCP Committee" in short)' to be formed comprising the following members

Chief Executive Officer-	Coordinator
Deputy Chief Executive Officer- Operations	Member
Deputy Chief Executive Officer- Credit	Member
Chief Risk Officer-	Member
Chief Operating Officer-	Member Secretary
Chief IT	Member

The committee is responsible for the overall assessment, monitoring and controlling the activities under the normal situations and in the event of crisis. In general, the committee shall be responsible for:

- Prioritizing the critical business functions

- Declare the disaster and guide for the prompt disaster management
- Works with the bank's Emergency Response Team to officially declare a disaster, and start the Disaster Recovery/ Business Continuation process to recover bank/ branch's business functions at an alternate site.
- Alert bank's Senior Management/ BOD that a disaster has been declared.
- Assist in the development of an official public statement concerning the disaster. The bank's spokesperson is the only individual authorized to make public statements about organization affairs.
- Monitor the progress of all Business Continuity and Disaster Recovery teams daily.
- Present Business Continuity Plan recovery status update to Senior Management/ BOD regularly.
- Interface with appropriate work management personnel throughout the recovery process.
- Provide on-going support and guidance to the recovery teams and other supporting personnel.
- Review staff availability and recommend alternate assignments, if necessary.
- Review and report critical processing schedules and backlog work progress, daily.

b. Emergency Response Team/Recovery Team

Emergency response team is led by Deputy Chief Executive Officer looking the operations of the Bank. The team member would be as below:

Deputy CEO-Operations	Coordinator
Chief Operating Officer	Member
Chief- IT	Member
Chief-Human Resources	Member
Chief/Head General Administration-	Member
Head-BOD	Member Secretary

The key functions of the team are as below:

- Regularly update the prevailing and probable situations to BCP Committee.
- Assign job to the different departments or staffs at the time of crisis handling
- Regularly conduct the test about the crisis handling, system drilling, disaster management and system fall over
- Train the staffs on the disaster management and crisis handling

- Identify, record and inform the evacuation spaces at head office and branches
- Monitor the branch preparedness on the business continuity and disaster management
- Monitor and ensure the implementation of BCP and Disaster Management Framework
- Inspecting the physical structure and identifying areas that may have sustained damage.
- Expanding on and/or revising the findings of the Preliminary Damage Assessment.
- Providing management with damage assessment reports and recommendations.
- Updating the information and needful precautions to the BCP Committee, Senior Management, Customers, Vendors/Contracts, Media in coordination of Spokesperson of the bank, regulatory agencies and other stakeholders, if necessary
- Coordinating, submitting, and tracking any and all claims for insurance.

c. Executives, Department Heads and Branch Managers

- Regular update that department and branches are in full compliance of this framework
- Get the instructions and information of Emergency Response Team and execute accordingly
- Be always in touch at the time of crisis with the Emergency Response Team for the actions to be done
- Ensure that the staffs under own responsibilities are safe at the time of crisis
- Ensure that customers under our functional scopes are safe at the time of crisis
- Ensure that the assets, documents and information are safe at the time of crisis

d. All Staffs

- Be safe at first
- Update own status first to the supervisor
- Get updated information from supervisor and act accordingly as per the instructions
- Be in touch and act for the safekeeping of bank's assets, documents, information and customers
- Act as instructed by supervisor

e. Other Key Departments' Functions

i. Human Resources Department:

- Notifying and coordinating on the employee injury or fatality with the family members and bank management.

- Coordinating on the medical treatments and recovery of employees
- Update the overall status of employees on their injury and safety status
- Ensuring the processing of all life, health, and accident insurance claims as required.
- Coordinates for the temporary employee arrangements as needed

ii. General Administration Department

- Arranging for the availability of necessary office support services and equipment.
- Tracking all cost related to the recovery and restoration effort.
- Coordinating with the vendors to schedule specific task for the repairs and restorations.
- Taking appropriate actions to safeguard equipment from further damage or deterioration.
- Coordinating with the department for relocations to the recovery sites.
- Assuring that arrangements are made for meals and temporary housing facilities, when required, for all recovery personnel.
- Other general administrative works for restoration of business to the normal condition

iii. Information Technology Department

- Activating the IT Technology Recovery Plan
- Managing the IT disaster response and recovery procedures.
- Mobilizing and managing IT resources.
- Coordinating all communications related activities, as required, with telephone & data communications, PC, LAN support personnel, and other IT related vendors.
- Assisting, as required, in the acquisition and installation of equipment at the recovery site.
- Ensuring that cellular telephones and other special order equipment and supplies are delivered as requested.
- Participating in testing equipment and facilities.
- Participating in the transfer of operations from the alternate site as required.
- Coordinating Disaster Recovery/IT efforts between different departments in the same or remote locations.
- Training Disaster Recovery/IT Team Members.

5. Declaration of Crisis/Disaster

All abnormal events or situations do not necessarily require declaring crisis. Based upon the probability of events and impact of that situation; crisis should be declared. Declaration of crisis is not based upon the specific rule; instead it is based upon best judgment. General idea can be taken with the help of the following matrix:

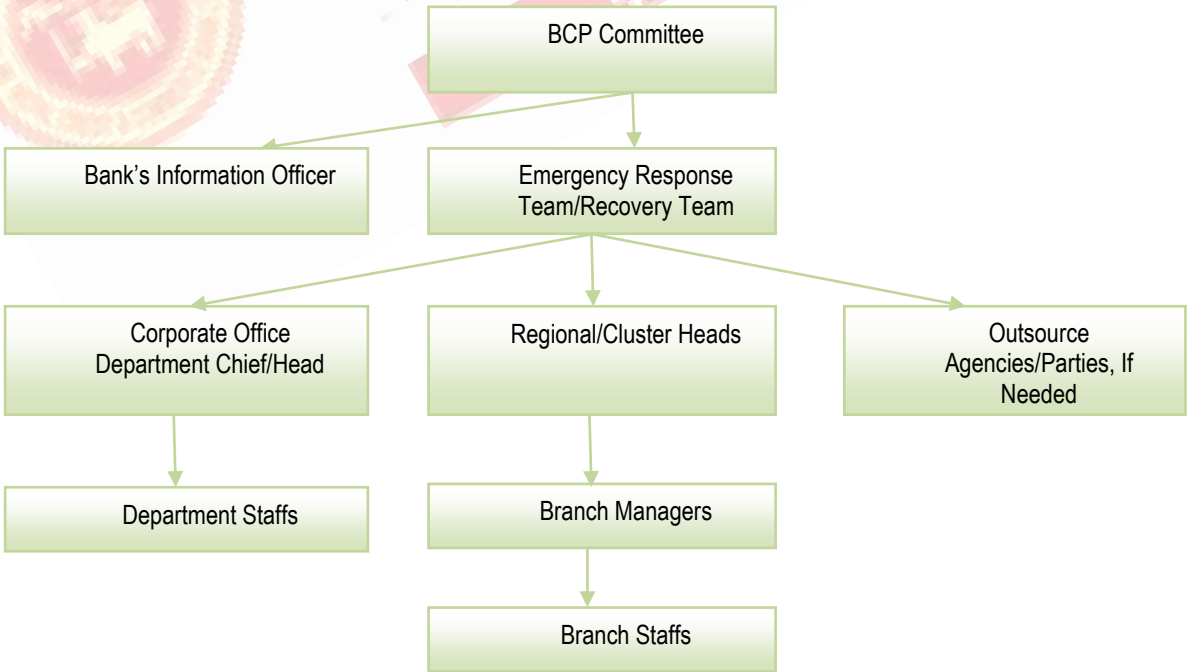
CRISIS EVENTS MATRIX		PROBABILITY	
		LOW	HIGH
IMPACT	LOW	IGNORE	NORMAL PROCEDURES
	HIGH	BE ALERT & PLAN	CRISIS SITUATION

Chief Executive Officer declares the events of crisis through appropriate means of communication. Board of Directors shall acknowledge the crisis declaration on its subsequent meeting. CEO may consult to Chairman for taking appropriate decision on crisis declaration and guidance.

The event of crisis can be in specific geography, district and region or as a whole Country. Upon declaration of crisis or disaster situation, structure created for crisis management will be functional.

6. Communication Tree/Channel

Upward and downward communication is most important on crisis handling. Effectiveness of business continuity and disaster recovery depends on how promptly and effectively information is communicated. Communication can be by means of phone, e-mail, SMS, hotline, website, public media or other available means. The communication channel shall be as below:



7. Business Continuity and Disaster Recovery Procedures

7.1 Phase of Disaster Recovery

The activities necessary to recover from disaster or disruption will be divided into four phases. These phases will follow each other sequential activities.

A. Disaster Occurrence

The beginning with the occurrence of the disaster event and continues until a decision is made to activate the recovery plans. The major activities that take place in this phase includes: emergency response measures, notification, damage identification and declaration of the disaster.

B. Plan Activation

In this phase, the Business Continuity Plans are put into effect. This phase continues until the alternate facility is occupied, critical business functions reestablished and computer system service restored to bank/ branch/ department. The major activities in this phase include: notification and assembly of the recovery teams (Emergency Response Team), implementation of interim procedures, and relocation to the secondary facility/ backup site, and re-establishment of data communications.

C. Alternate Site Operations

Alternate operations are established and continue until the primary facility is restored. The primary recovery activities during this phase are backlog reduction and alternate facility processing procedures.

D. Transition to Primary Site

It consists of any and all activities necessary to make the transition back to a primary facility location.

7.2 Recovery Priorities

Based upon the sensitivity and severity of losses, business functions are prioritized for the immediate recovery at the secondary locations. Safety and security would be on the top priority. Information must be collected at first whether staffs, customers and other visitors are safe or not. All the people must be shifted on safe place or the evacuated place. Information Systems shall recover IT functions based on the critical branch/ departmental business functions and defined strategies. Emergency response team prepares the priority list after the incident and advises to all concerned through effective communication channel that what are in general priorities that all concerned have to take care.

7.3 Recovery Procedures

Recovery procedure is the plan that describes the specific activities and tasks that are to be carried out in the recovery process for normal business continuation. Each activity has a designated team member

who has the primary assignment to complete the activity. Most activities also have an alternate team member. The activities will only generally be performed in this sequence.

Phase- I

i. Disaster Occurrence

a) After disaster occurs, quickly assess the situation to determine whether to immediately evacuate the building or not, depending upon the nature of the disaster, the extent of damage, and the potential for additional danger.

b) Quickly assess whether any personnel in your surrounding area are injured and need medical attention. If you are able to assist them without causing further injury to them or without putting yourself in further danger, then provide what assistance you can and also call for help. If further danger is imminent, then immediately evacuate the building.

c) If appropriate, evacuate the building in accordance with your building's emergency evacuation procedures. Use the nearest stairwells. Do not use elevators.

d) Outside of the building meet at open space. Do not wander around or leave the area until instructed to do so.

e) Check in with your department manager for roll call. This is important to ensure that all employees are accounted for.

ii. Notification of Management

a) Department Head/ Branch Manager inform the members of the BCP Committee and notify the senior management if they have not been informed.

b) Depending upon the time of the disaster, personnel are instructed what to do (i.e. stay at home and wait to be notified again, etc.)

iii. Preliminary Damage Assessment

a) Contact the Emergency Response Team to determine responsibilities and tasks to be performed.

b) If the bank/ branch Emergency Response Team requests assistance in performing the Preliminary Damage Assessment, caution all personnel to avoid safety risks as follows:

i. Enter only those areas the authorities give permission to enter.

ii. Ensure that all electrical power supplies are cut to any area or equipment that could possess threat to personal safety.

iii. Ensure that under no circumstances power to be restored to computer equipment until the comprehensive damage assessment has been conducted, reviewed, and authority to restore power has been expressly given by the top level management of the bank.

c) Inform all team members that no alteration of facilities or equipment can take place until the Risk Management representatives (Senior Level Management) have made a thorough assessment of the damage and given their written agreement that repairs may begin.

d) Instruct the Emergency Response Team to deliver the preliminary damage assessment status report immediately upon completion.

e) Facilitate retrieval of items (contents of file cabinets -- cash box, security codes, network backup tapes, control books, etc.) needed to conduct the preliminary damage assessment.

f) Ensure that administrative support is available, as required.

Phase- 2

i. Declaration of Disaster and Plan Activation

a) BCP Committee declares the disaster situation. Emergency Response Team should wait for notification from BCP Committee that disaster has been declared and other teams are to start executing their Business Continuity Plans and relocate to their Alternate Business Site.

b) Review the recovery strategy and action plan with the team. Instruct to the emergency response team for immediate actions for the recovery of crisis impact.

ii. Business Continuation and Recovery

a) Disaster recovery team contacts critical employees and tells them to assemble at the alternate site. If the alternate site is a long distance from the primary site, then individuals should make their own travel arrangements to the alternate site.

b) Non-critical employees should be instructed to stay at home, doing what work is possible from home, until notified otherwise.

c) In the event of a disaster that affects telecommunications service regionally, the team should instruct critical employees to proceed to the alternate site even if they have not been contacted directly.

d) If allowed access to the primary site to retrieve vital records and other materials, perform some pre-planning to determine what is most important to retrieve. This may be necessary since the time you may be allowed access to the primary site may be minimal. Make arrangements to transport the materials and record to the alternate site.

e) Map out locations that can be used for workspace. This should include unused offices and cubicles, conference rooms, training rooms, lunch/break areas, and open space in hallways or in other areas.

f) Obtain additional tables and chairs, either from the office or from outside rental agencies to provide additional workspace. Place in any available open areas, but be cautious of not blocking exits for fire evacuation purposes.

g) Determine flexible working schedules for staff to ensure that client and business needs are met, but also to enable effective use of space. This may require that some employee's work staggered shifts or may need to work evening or nightshifts.

h) Develop prioritized work activities, especially if all staff members are not available.

i) Prepare a list of phone extensions which your staff will be temporarily using and provide this list to the alternate site switchboard attendant.

iii. Restoring Data Processing and Data Communications with Primary or Secondary Backup Data Center

a) Contact the bank's Emergency Response Team to determine when the data center is to be recovered, if affected by the disaster. Also, discuss when data communications will be established between the primary or secondary backup data center and your alternate site.

b) If your alternate site is another branch office, determine if that site has access to the computer systems. If so, work with local office management to determine how workstations can be shared between personnel from their groups/departments. This may involve using flexible hours or multiple shifts for your personnel.

c) Discuss with the bank's emergency response team when and how replacement of PC and/or terminals will be provided at the alternate site and when they will be connected.

d) Communicate the IT recovery status to all personnel who regularly use the systems.

Phase- 3

Alternate Site Operations

a) Communicate with customers regarding the disaster and re-solicit phone contacts (in conjunction with the Organization Communications Team)

b) Acquire needed vital documents

c) Get access on missing documents or files and reconstruct, if necessary

d) Determine priorities for work backlogs to ensure the most important backlogged tasks are resolved first.

e) Report the backlog status to BCP Committee on a regular basis.

f) If backlogs appear to be very large or will take a significant time to recover, determine if temporaries could be used for certain tasks to help eliminate the backlogs. If justified, arrange for temporaries to come in.

g) The manpower in respective branch/ department in conjunction with designated delivery/courier services will distribute mail to all bank alternate business sites. Due to the possibility of multiple

alternate business sites and the additional travel time required for mail service activities, the number of mail pickups and deliveries could possibly be decreased from the normal daily routine to once daily.

Phase- 4

i. Transition to Primary Operations

Responsibility: Emergency Response Team

a) Coordinate with the bank's Emergency Response Team to determine when branch/ department will be relocating back to the primary site. Verify that they have a schedule to ensure that telephone and data communications are rerouted accordingly.

b) Discuss when and how PC's, terminals and printers, if brought into the alternate site, will be re-installed, moved back to the primary site and re-installed.

ii. Terminating Alternate Site Procedures

a) Determine which alternate site operating procedures will be suspended or discontinued and when.

b) Communicate the changes in procedures to all concerned staffs.

c) Determine if additional procedures are needed upon return to the primary site, such as to continue resolving work backlogs.

8. Sensitive Records Backup and Restoration

All sensitive records of branches and departments that could be affected by a disruption or disaster are maintained and controlled by either Emergency Response Team. The team may instruct to other departments to store the documents and information through written instructions like: IT for data backup, GAD for legal ownership documents, credit for credit related security documents etc. The team may instruct to store the documents and backup information on site or off site from office premises. BCP Committee also instruct for the necessary task and procedures for sensitive record and information backup. BCP Committee may list out the most critical and sensitive documents and information for storing safely to be protected in the condition of crisis and disaster.

8.1 Restoration of Hardcopy Files, Forms, and Supplies

In the event of a facilities disruption, critical records may be destroyed or inaccessible. In this case, the last backup of critical records in the secure warehouse would be transported to the secondary location or facility. The amount of critical records, which would have to be reconstructed, will depend on when the last shipment of critical records to the offsite storage location occurred. BCP Committee will arrange

the frequency of rotation of critical records to the offsite storage site. The following categories of information can be exposed to loss:

a) Any files stored on-site in file cabinets and control file rooms.

b) Information stored on local PC hard drives.

c) Any work in progress.

d) Received and un-opened mail.

e) Documents in offices, work cubes and files.

f) Off-site records stored in the Records Warehouse (if this is not a secure, hardened facility).

8.2 On-line Access to Bank's Computer Systems

In the event of a facilities disruption, the IT should assist in re-establishing connectivity to the bank's branch/ department and to establish remote communications to any alternate business site location. If the data center is affected by a disaster or disruption, the IT Disaster Recovery Plan mentions the recovery procedures at a pre-determined alternate site. Services covered would include; phones, cellular phones, communications including Radio Modem and all other services required for restoring limited emergency service to the organization. In this case, data communications will be rerouted from the data processing hot or cold site to the respective alternate business site locations.

The representatives should understand, and enter here, what the recovery timeframe is for systems recovery (i.e. will have critical systems restored within hours or days) and what the strategy is for acquisition, installation, and connection of PC's/terminals. Acquisition and recovery of critical standalone personal computer capabilities should also be considered. It should also understand the IT strategy for recovery of applications, those on desktop systems, which BCP Committee relies on.

8.3 Mail and Report Distribution

During the time that bank's branch/ department operations are run from the secondary facilities, output reports and forms will have to be delivered to that location. The data center may or may not have the same print capability if the disruption affected the data center as well, so it may be necessary to prioritize printing of output.

9. Evacuation Plan

Head office and individual branches shall have the evacuation strategies which will be communicated to the staffs clearly. Evacuation may need at the time of earthquake, fire, floods, attacks etc. Each floor of Head Office and branches shall have floor plan displaying the main entrance, emergency exit, fire alarm, emergency meeting hall and other security places which are to be used in the critical situation. Security guards shall be oriented to make help to the disable persons and guide the other persons in

case of emergency. GAD update the plan and ensure the properly display in the braches and head office.

There will be a defined place in each branch and head office for evacuation of office premises on emergency. Evacuation of office premises shall be made with proper security measure like: cash vault is closed, teller cash drawer is closed, key security documents are safely locked, staffs inside office are well informed, main door is closed etc. Evacuation place shall be free from the risk/events of office premises.

While evacuating the office premises, Branch Manager, Department Head or Functional Officer must ensure that all staffs are come out from the office. General duties while evacuating the works stations are as follows:

Department/Person	Task
Executives	Ensue all staffs under supervision are informed the incidents and noticed to evacuate the place
Department Head	Ensue all staffs are informed the incidents and noticed to evacuate the place
Department Staffs	Ensure security items are safely stored
Branch Manager	Ensue all staffs are informed the incidents and noticed to evacuate the place
Operation In-Charge	Ensure all the securities and cash are safely kept on position as it where it. Cash vault is locked. To the best possible all teller cash to be kept on fire proof cabinet.
Teller or Head-Teller	Cash is in locked position

While handling and evacuating the working place, following basic issues have to be ensured first on disaster management process

Key Critical Measures/activities	Yes/No	Remarks
Are employees safe and can work on confidence		
Are the customer safe		
Can the basic banking needs like: confidentiality, security, accuracy, reliability and service be ensured		
Is the IT Infrastructure adequate to provide service		
Is the network working properly and protected from emergency crisis		
Are the critical activities identified to start		

Whether regulatory authorities or national law restrict or mandate to run the activities		
Have we got proper administrative and operating consent internally from competent authority		
Does the CCTV work properly		
Whether access points (doors, fire doors, windows) provide the required level of protection.		
Ensure that the facilities for storing vital records, sensitive data and other items of value are in accordance with minimum standards.		

10. Continuity and Recovery Plan on Information Technology (IT)

10.1 Risk Identification and Assessment

The Bank operates in highly automated environment in terms of information technologies and communication systems which enables the bank to deliver quality services to their customer. The Bank is constantly innovating to meet the business objectives by providing essential and unique services to their customers. Despite all business precautions, interruption does occurs without any pre-notification so in order to mitigate those unnoticed interruption which we call the risk we need to implement the BCP for the Bank.

Some of the possible risk events come unnoticed (unwarned) and most of them never happen even though, the Bank needs to prepare and be able to respond the event when it does occur.

It is the exercise of identifying and analyzing the potential vulnerability and threats. The identified source of risk can be:

- System/Technical Failure e.g. system and equipment failure, use of pirated applications, manipulation of data, system reboot, hacking, Phishing, Virus attack etc.
- Natural Disasters e.g. Fire, Flood, Earthquake etc.
- Human Made Issues e.g. riots, crime, terrorism, theft etc
- System Supply Failure

Below we present the magnitude of risk and the probability of its occurrence:

Identified Risk	**Possibility**			**Impact**
	Low	Average	High	
System /Technical Failure				High
Natural Disaster				High
Human Made Issues				High
System Supply Failure				Average

The main goal of Risk assessment is to identify, evaluate and manage the risk in order to eliminate or minimize the consequences of any unplanned events, during the normal operation of the Bank. Planning is done for both prevention and control.

Risk Identification assist on finding the probability and the size of the risk. This introduces exact threats the industry is facing and the estimated exposure together with the contingency and mitigation actions required.

Risks are correlated with the security of physical infrastructure and personnel practices which have a direct impact on the day to day operation of the critical applications that is essential for our business. Measured risks and the compliance procedures to mitigate, are illustrated as below:

Control Objectives	Control Technique	Compliance Procedures
1.Security on Natural Disaster		
Primary Data Center is at 2nd Floor of the building. DRC is at the Data Room of the Ohm Data Centre, Bhairawaha	-PDC is at 2nd floor of the building. -The building/ PDC is covered by lightening arrester .Separate fire extinguisher for building and PDC -Fire extinguisher/ lightening arrester at FDC	-Minimizes the chance of flooding -Need to review the status/conditions by IT and GSD -Need to review the status by IT Team along with the Ohm Data Centre Representatives -The Team at Ohm Data Centre is responsible for all the Security Risk.
2. Physical Security		
The Computer / Data and telecommunications equipment of PDC are secured Fire Alarm System	-PDC/DRC contains the equipment's solely of IT department. -Closest of Cable tray, Electric tray or any other are adequately controlled -Physical restriction to enter at PDC /DRC -Automatic fire alarm system installed, separate for DC and HO building	-Need to confirm no computer and telecommunications (related to Data Analytics) equipment's exist outside a secured Data Center -Need to determine whether closest are properly closed/locked in case we found any then GSD/ITD will remedy it. -Need to ensure the door

Control Objectives	Control Technique	Compliance Procedures
		system are locked with Access Control (log book are maintained) -Need to ensure only authorized individual's posse's keys or password to Access Control -Rehearsal required
3. Power System		
Besides CT line, available of generator and UPS for backup system	-Consists of primary and secondary generator at PDC/DRC for the power backup -PDC have primary and secondary UPS system -DRC have no separate generator, HO Building generator is used for power backup and UPS capacity of max five hours backup is being used	-GSD at DC and Ohm Data Centre representative at DRC will ensure both the generator are workable and servicing is conducted timely -Output and input of both the UPS of PDC need to be checked and servicing should be conducted on schedule -Need to ensure servicing are done on timely and GSD will be looking after this.
4. System Connectivity		
CBS and other services are in centralized architecture. Making the system available and minimizing the downtime, primary and secondary branch connectivity is available	- Primary link at PDC is from two different paths at Building. -Have primary and secondary intranet connectivity from two different ISP at each Branch -Network equipment's of the Branch automatically detect the secondary link if primary link goes down. Like-wise communication equipment's at DC are in high availability mode, if one equipment fails another	-Need to review the conditions of the equipment's time-to-time -AMC needs to be done with Netfiniti Pvt. Ltd for the communications equipment's

Control Objectives	Control Technique	Compliance Procedures
	equipment automatically take-over the responsibility -Extra network equipment (router) are kept at Head Office as a replacement unit for the Branch	
5. Physical Access Lists and Visitor Logs		
Controls are in place to ensure the unauthorized access to safeguard critical equipment's	-Automatic access lock system at PDC -Vendor/ consultant/ support people are allowed to enter inside the room under the principle responsibility of one of the people who is authorized for the access at PDC	-Need to maintain the visitors log book and need to be review
6. Password Protections		
Logical controls over Server and Communications equipment's	Access control are in place for unauthorized accessed at servers and communication equipment's of PDC	Need penetrating testing for security breaches
7. Anti-Virus		
Antivirus installed	ESET NOD32 antivirus is being installed at all the servers and PC's	Need to review

10.2 Impact Analysis in the Business (IAB)

IAB is essentially the process of identifying the critical business functions and the losses/effects if these functions are not operational.

Steps to find the impact analysis in the Business

- Finding how long the function could be inoperative without any impact or losses.
- Categorize the vital functions relating the overall business strategy.
- Find out whether it has direct impact on the customer.
- Finding whether it create legal/regulatory issues.

Requirements for recovery after disruption

- Resources and records are required to continue the business functions.
- The time and efforts required to recreate up-to-date data from the backups
- Upon which external business/suppliers/vendors it would be dependent.

Based on above steps and requirements we can classify business into three parts

a) Critical Functions
b) Essential Functions
c) Necessary Functions

Critical Functions

If these business functions are interrupted or unavailable for some time, it can completely jeopardize the business and cause heavy damages to the Bank such as

S/N	Critical Applications	Dependency	Impact
1	CBS PDX to Route ATM transaction	Mercantile Office System Pvt. Ltd (the vendor)	***Very High***

Essential Functions

Those functions, whose loss would seriously affect the Bank's ability to function for long,

S/N	Essential Applications	Dependency	Impact
1.	ATM Switch	Nepal Investment Bank Limited	***High***
2.	Email System	Open source at ITD responsibility	***High***
3.	SWIFT System	SWIFT	***High***
4.	NCHL-ECC	Nepal Clearing House	***High***
5.	Mobile Banking/Bank Smart	F1Soft International	***High***
6.	Counter Bill Payment	F1Soft International	***High***
7.	Internet Banking	Mercantile Office System	***High***

Necessary Functions

The bank can continue functioning; however, absence of these functions would limit the effectiveness, to a great extent.

S/N	Necessary Applications	Dependency	Impact
1.	HRIS	Rigo Nepal	***Low***

2.	Intranet System	In-House	***Low***
3.	Fixed asset and Inventory Management system	Swift Management	***Low***

**The list shall be updated and approved on a separate paper as when changed*

Based on the recovery needs, the Bank has defined standard recovery time frames for the above business functions:

S/N	Task	Recovery Time
1.	Critical	***Within 5 hours***
2.	Essential	***Within 1 Day***
3.	Necessary	***Within 2 Day***

Strategy Plans

BCP include following strategies:

- Prevention
- Response & Communication
- Resumption Site
- Recovery Site

Prevention

Strategies for prevention reduce the probabilities of threat to occur or reduce its impact. Having these measures in place is always more cost-effective than attempting for recovery after the interruption. The Bank shall aim to cover as many as risks to identify and to establish preventive controls, so that the recovery strategy has to work out only on the residual risks. A wide variety of such controls exist, some of the common ones are described below:

- Security at the premises
- Access Control at Data Center for Internal/External People
- Adequate and well equipped IT resources
- Access Control on Software/Network Device
- Enough resources for Recovery on worst case

10.3 Response & Communication

The first reaction after an interruption of any service would be to inform the relevant people about the interruption. If there is a prior warning about the impending interruption, then this should be immediately informed by the monitoring team.

Timely notification is important, since it may provide an opportunity to stop any further damage. In a situation where there is an adequate time to perform a primary preventive function such as a shutdown, a switchover or an evacuation, it may even completely prevent damage.

Such controls are diagnosis by the assigned team member by continuously scanning/monitoring network, servers/communication devices and power backup or collection of information from external sources about natural calamities. Source of information for possible interruption are as below:

S/N	Issues	Source of Information	Monitoring Team
1.	Natural Calamities (such as hurricane, lightening, earthquake)	Online News, External Information	*An User from IT Department who prepare/ submit the System Health-Check report Daily*
2.	Application	Monitoring System	
3.	Database	Monitoring System	
4.	Network	Monitoring System	
5.	Power Backup	Monitoring System	
6.	Virus	Monitoring System	

10.4 Resumption Site

This location is different from the PDC i.e. having normal business facility. It is the location to ensure resumption and subsequently coordinate the recovery activities. The center does have adequate communication facilities and required resources to support the activities that are supervised by Ohm Data Centre. For the resumption of business process, the Bank has outsourced DRC at Ohm Data Centre Bhairawaha.

The first decision to be taken is whether the critical operations can be resumed from the normal business site or should be resumed from an alternate site. In such situations, when access to the primary site is denied or the site is fully damaged beyond use, the operations are moved to an alternate site for business continuity. This site is configured with the followings facility to support for the BCP:

- The site is configured similar to PDC with low resource capability and is the Bank '***DR Site***'
- The Bank has set the ***Recovery Point Objective (RPO)*** threshold. It is from the exact point from where the business has been interrupted i.e. loss of zero percent data
- The Bank has set Five (5) hours ***Recovery Time Objective (RTO)*** threshold, in-case of failure of primary site.
- In case, the Banking database of PDC become corrupted the online replicated data of DRC will be also affected. In such case the Bank the RPO is 3 hours back.

It is possible that the Bank can choose either the automatic or manual mode in case of PDC failure for service resumption from FDC.

10.5 Recovery Site

At the site of recovery, the ***Critical*** data is replicated online using Always On feature that is inbuilt in SQL Server. If when the critical system (CBS) is not able to be functional from the PDC the recovery site can be used for making CBS available. From this site, the limited users are allowed to access the system with following facilities to support for the BCP:

- This site is configured with very low resources and is the '***DR Site'*** of the Bank
- The Bank has set the ***Recovery Point Objective (RPO)*** threshold. It is from the exact point from where the business has been interrupted i.e. loss of zero percent data
- The Bank has set five (5) hours ***Recovery Time Objective (RTO)*** threshold, in-case of failure of both PDC.

10.6 Testing BCP

The dates of testing, disaster recovery scenario, and plans for each scenario should be documented. Maintenance involves record of scheduled review on a daily, weekly, monthly, quarterly, yearly basis; reviews of plans, teams, activities, tasks accomplished and complete documentation review and update.

The disaster recovery plan developed thereby should be tested for efficiency. To aid in that function a test strategy and corresponding test plan should be developed and administered. The results obtained should be recorded, analyzed, and modified as required.

Cases for testing BCP

The Bank has prepared broad guidelines/ test case for determining the capability of the BCP. Below are the cases for the rehearsal:

S/N	Drill Case	Expected Result	Expected Impact
1	Failure of primary server running Core Banking System (CBS)	CBS should be automatically switched to secondary server or any available Nodes	There should not be downtime on any Banking services
2.	Failure of secondary server running Core Banking System (CBS)	CBS should be automatically switched from primary server	There should not be downtime on any Banking services
3.	Failure of both server running Core Banking System (CBS) at PDC	Core Banking System (CBS) should be operated from Data recovery Centre (DRC). Other services should be running from Primary Data Centre (PDC)	There will be maximum of 5 hours down time for all services

S/N	Drill Case	Expected Result	Expected Impact
		a. E-Mail b. E-Banking c. ATM d. Other Utility Services (Mobile Banking, Counter Bill Payment)	
4.	Failure of primary network device of Primary Data Centre (PDC)	Connectivity should resume via secondary network device of Primary Data Centre (PDC)	There should be no downtime
5.	Failure of secondary network device of Primary Data Centre (PDC)	Connectivity should be resumed from primary network device	There should be no downtime
6.	Absence of primary connectivity from POP A of first ISP at Primary Data Centre (PDC)	Entire traffic of POP A should automatically route through secondary POP B of first ISP	There should be no downtime
7.	Absence of secondary connectivity from POP B of first ISP at Primary Data Centre (PDC)	The traffic should be routed through POP A of first ISP	There should be no downtime
8.	Absence of primary ISP (POP A & B) at Primary Data Centre (PDC)	All the traffic of branches should route from the secondary ISP	Service and Branches which are depended upon Primary ISP will be interrupted.
9.	Entire PDC failure	All the network traffic of branches should route to DRC	Branches should get the access to CBS within 5 hours except HO. Gradually other services will be accessible except SWIFT and ATM Card. These services shall take few days since there is no online replication facilities for these services

Testing frequency

Testing frequency of the component of business continuity based on critical of a process is defined as below:

S/N	Component	Impact on Process	Frequency
1.	Network Equipment	Low	Quarterly
2.	Servers	High	Quarterly
3.	Backup Database	Low	Monthly
4.	Business operations from DRC	Very High	Yearly

10.7 System Change Management

A change is defined as anything that transforms, alters, or modifies the operating environment or standard operating procedures of BCP that have potential to affect the stability and reliability of IT-supported services and disruption of business activities of the Bank.

If any changes required that should be recorded and approved in the Annexure of '*Change Management Procedures*'. It should cover all the planned, unplanned, emergencies changes including the maintenance and minor updates.

Standard Operating Procedure

S/N	Equipment	Description
1.	***Uninterruptable Power Supply (UPS)***	• Check the Power Cables both Input/output • Check the Power on the main supply • Check the current settings • Check the indicators, dash-board for error code/ description • Follow the instruction on the manual as per the error code • Write down time and date if any change to the configuration has been made or if the device has been restored to factory settings. • Contact to vendor if the issue has not been resolved
2.	***Battery Pack***	• Check the batteries connected power cables of charger/ups

S/N	Equipment	Description
		• Check whether batteries are continuously charging or not • Check the input/output voltage • Check the health of the batteries • If any batteries found unhealthy on the series, recommend for the replacement • Write down time and date if any change made • Contact to vendor if the issue has not been resolved
3.	***UPS Power Bypass Switch***	• Switch-on Bypass Switch if the battery pack found faulty • Check the Output Power Cable
4.	***Power Distribution Unit (PDU)***	• Check the Main Power supply • Check the Power Cables • Check the indicators • Fix the issue if found or change the PDU if found faulty
5.	***Firewall/ Router***	• Check the Power Cables • Check the current settings of the device • Check the light indicators for error findings • Monitor the resource utilization by the devices • Consult the Instruction manual if any changes required • Write down time and date if any change to the configuration has been made or if the device has been restored to Factory Settings
6.	***Media Converter***	• Check the Power Cables • Check the Network Cables • Check Indicators for error description (FSD/FL/PWR & TL/100/FD)

S/N	Equipment	Description
		• Contact to ISP and lodge the issues for maintenance & support
8.	***Storage***	• Check the Power Cables • Check the Network Cables • Check configuration of device • Check drive bays, Hard Disks • Check Indicators for error / description • Consult the Instruction manual • Write down time and date if any change to the configuration has been made or if the device has been restored to Factory Settings
9.	***Server***	• Check Power Cables • Check the Network Cables • Check the VGA/Data Cables • Check the status (Hardware, OS) • Check indicators/beeps for error descriptions • Check configuration of the device • Consult the Instruction manual • Write down time and date if any change to the configuration has been made or if the device has been restored to Factory Settings
10.	***IP Camera***	• Check Power / Adaptor Cables • Check the Network Cables • Check the visibility • Make sure the camera is recording the video • Check configuration of the device • Consult the Instruction manual • Write down time and date if any change to the configuration

S/N	Equipment	Description
		has been made or if the device has been restored to Factory Settings
11.	***Access Control Device***	• Check Power / Adaptor Cables • Check the Network Cables • Check configuration of the device • Consult the Instruction manual • Write down time and date if any change to the configuration has been made or if the device has been restored to Factory Settings
12.	***Fire Extinguisher***	• Check the seal / tag • Check the validity dates (expiry) • Check the function, lock and mount • Check the weight • Consult the Instruction manual • Write down time and date if any change to the configuration has been made or if the device has been restored to Factory Settings
13.	***Smoke Detector***	• Check functions • Check connections, connectors • Check warning beeper/alarms • Check configurations • Consult the instruction manual
14.	***Printer***	• Check the Power Cable • Check the data Cable/Network Cable • Check the Driver Compatibility • Check the status of Cartridge, replace if required • Check the font size/format in case of dot-matrix printer • Take the help of manual if required

S/N	Equipment	Description
		• Write down the time and date if any change on the configuration has been made
15.	***Connectivity***	• Check the power supply on MC/Router/Switch • Check the network cable from MC to router or Router to Switch • Check the network from faceplate to computer • Check the network card and its driver compatibility • Contact the service provider if required • If any changes on Router/ Switch, note down the changes made
16.	***Computer***	• Check the power supply • Check the operating system • Check the IP of the Computer • If any changes made, note down the changes made

List of Hosted Servers and Storage/ PDC Hosting Storages and Servers

The List of Application including the CBS and Swift along with auxiliary services hosted at PDC is listed below:

Core Banking				
S No	**Name of Server**	**IP Details**	**User Name**	**Password**
1	CBS Node 1	192.168.**.**	**********	********
2	CBS Node 2	192.168.**.**	**********	********
3	Windows Cluster	192.168.**.**	**********	********
4	Storage MGMT GUI 1	192.168.**.**	**********	********
5	Storage MGMT GUI 2	192.168.**.**	**********	********
6	Storage MGMT Service 1	192.168.**.**	**********	********
7	Storage MGMT Service 2	192.168.**.**	**********	********
8	CBS Node 1 IMM	192.168.**.**	**********	********

9	CBS Node 2 IMM	192.168.**.**	**********	********
10	Cisco 2960-X(MGMT SW)	192.168.**.**	**********	********
11	Cisco 3650(CBS SW1)	192.168.**.**	**********	********
12	Cisco 3650(CBS SW2)	192.168.**.**	**********	********

Virtual Machine 1				
192.168.**.**				
S No	**Name of VM**	**IP Details**	**User Name**	**Password**
1	AML Server	192.168.**.**	**********	********
2	DMAT Server	192.168.**.**	**********	********
3	HR Server	192.168.**.**	**********	********
4	ASBA Server(TESTSERVER)	192.168.**.**	**********	********

Virtual Machine 2				
192.168.**.**				
S No	**Name of VM**	**IP Details**	**User Name**	**Password**
1	Antivirus	192.168.**.**	**********	********
2	BankSmart Application	192.168.**.**	**********	********
3	BankSmart Database	192.168.**.**	**********	********
4	CounterBill	192.168.**.**	**********	********
5	IPS Server	192.168.**.**	**********	********
6	SharePoint	192.168.**.**	**********	********
7	BankSmart T2P	192.168.**.**	**********	********

Individual Servers				
S No	**Name of Server**	**IP Details**	**User Name**	**Password**
1	Email	192.168.**.**	**********	********
2	Active Directory	192.168.**.**	**********	********

3	Active Directory Backup	192.168.**.**	**********	********
4	Retirement Fund	192.168.**.**	**********	********
5	Intranet	192.168.**.**	**********	********
6	STORAGE MGMT	192.168.**.**	**********	********
7	Internet Banking	192.168.**.**	**********	********
8	Swift	**********	**********	********
9	Fixed Assets Management	192.168.**.**	**********	********
10	Pumori Test Server	192.168.**.**	**********	********
11	spstg	192.168.**.**	**********	********
12	COS	192.168.**.**	**********	********

Individual STORAGE at DC				
S No	**Name of Storage**	**IP Details**	**User Name**	**Password**
1	STORAGE QNAP	192.168.**.**	**********	********
2	STORAGE QNAP	192.168.**.**	**********	********
3	STORAGE QNAP	192.168.**.**	**********	********

Networking Devices at PDC				
S No	**Device**	**USED**	**USER**	**PASSWD**
1	FortiGate-100D	BRANCH-PVN	********	********
2	FortiGate-100D	BRANCH-PVN	********	********
3	FortiGate-200D	CORE	********	********
4	FortiGate-200D	CORE	********	********
5	FortiGate-200D	EXTERNAL-VPN	********	********
6	FortiGate-200D	EXTERNAL-VPN	********	********

DRC Hosting Server and Storages

The List of Application including the CBS hosted at DRC is listed below:

Servers and Storage at DR				
S No	**Name of Server**	**IP Details**	**User Name**	**Password**
1	DRServer1	10.80.**.**	**********	********
2	STORAGE MGMT	*********	*********	********

Networking Devices at PDC				
S No	**Device**	**USED**	**USER**	**PASSWD**
1	FortiGate-140D	HO-Branch-VPN	********	********

Records and Check Lists

Drill Case Record Sheet

S/N	Drill Case	Expected Result	Expected Impact	Drill Out-Come	Shortfalls

Pre/Post Rehearsal Confirmation/ Verification Sheet

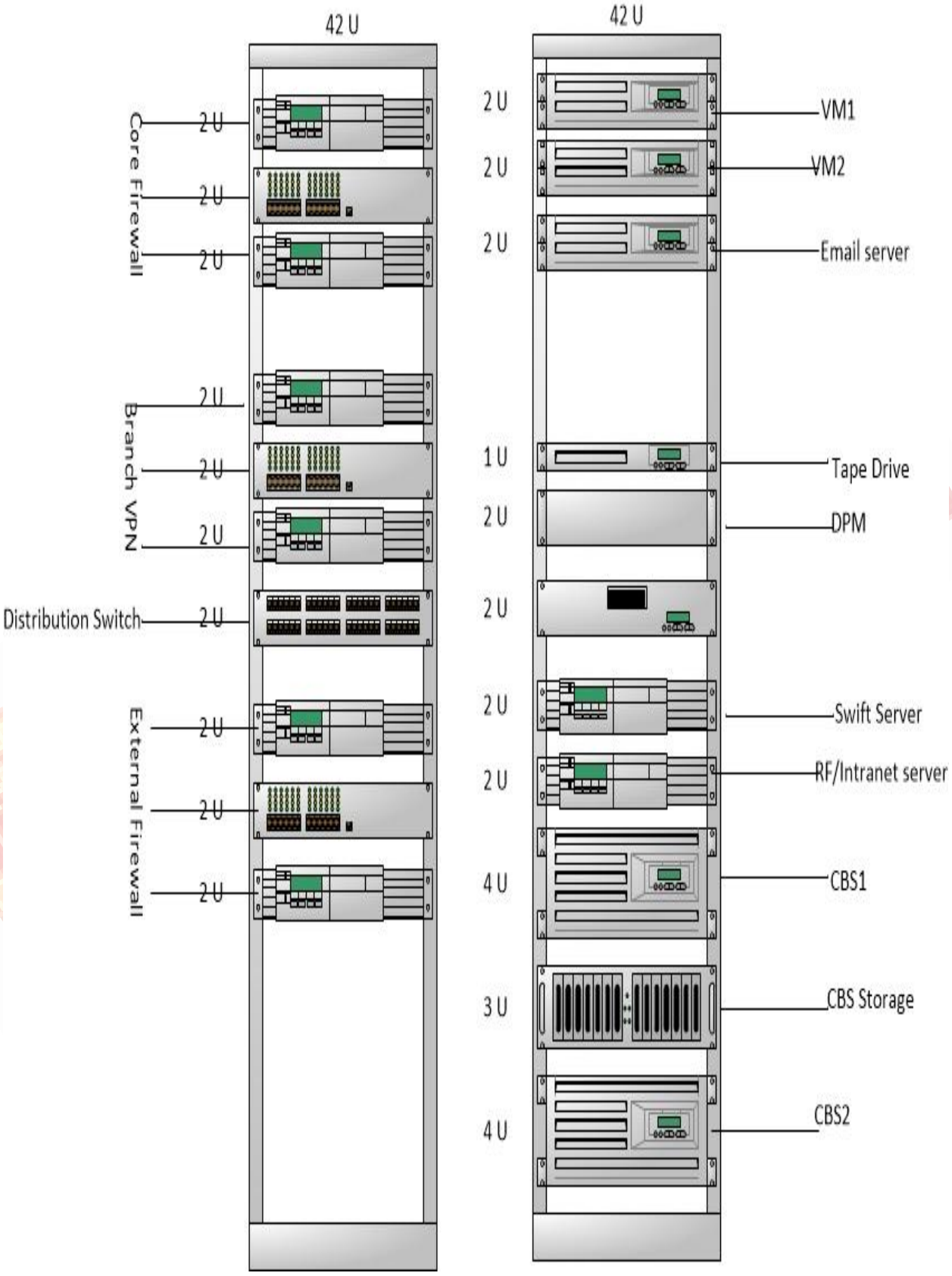
S No	Date/Time	Actions	Defense
1.	Date: Time:	**Cross-check the status of:** -Power: -Connectivity: -Server: -Communication Equipment:	
2.	Date: Time:	**Service Status before Switch-Over/Fall-Back of Site**	
3.	Date: Time:	**Switch-over/Fall-Back of Site**	
4.	Date: Time:	**Data Consistency-check, between the Sites** • *Day Started of:* • *Total transaction of the day:* • *Last Sequence number of the transaction:* • *Total Balance of financial Accounts:* • *Database Name:* • *Others:*	

S No	Date/Time	Actions	Defense
5.	Date: Time:	**Service Status after Switch-Over/Fall-Back of Site**	
6.	Date: Time:	**Network Routing Added/Deleted**	
7.	Date: Time:	**Source and Destination of the Applications**	
8.	Date: Time:	**Update/Change on Server**	
9.	Date: Time:	**Systems Available for Users/Customers**	

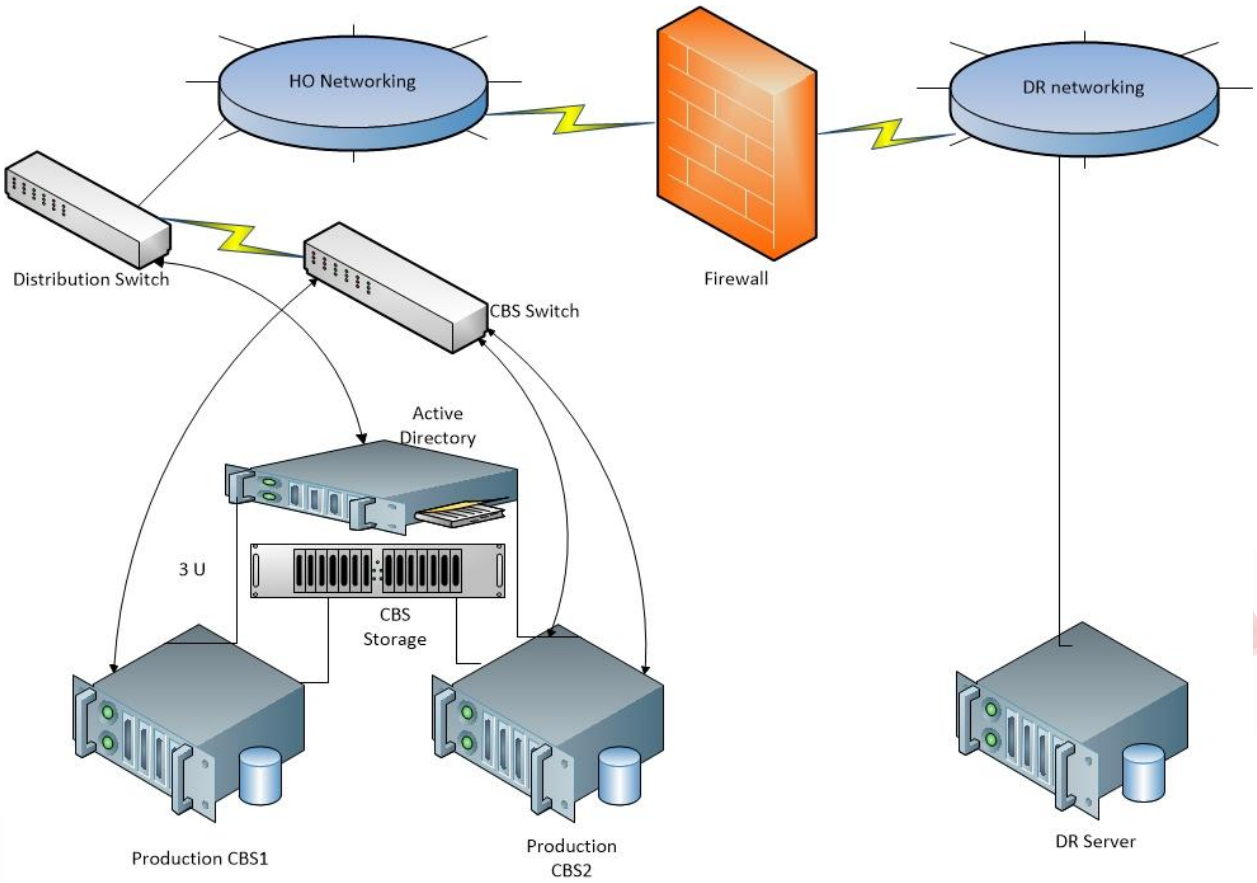
Data Recovery & Restoration Check list

S No	Parameters	Tick (√)	Remarks
1.	Review key concepts and prepare to backup date		
2.	Make the perquisite ready for running the system		
3.	Check the Operating System and Database on the server		
4.	Verify the system is logged in		
5.	Insert the external media where the latest backup has been backed		
6.	Confirm the latest data and copy on the server		
7.	Restore the database		
8.	Check the consistency of the data from every angle, between database date/time till disaster happened		
9.	Find-out the missing deposit/withdrawal transactions from the available vouchers/ cheques between the time		
10.	Find-out the missing electronic channels transactions from the available logs between the time		
11.	Reconcile the customer/financial accounts from the available records		
12.	Confirm with the Head BCP/Higher Management		
13.	Make the CBS system available		

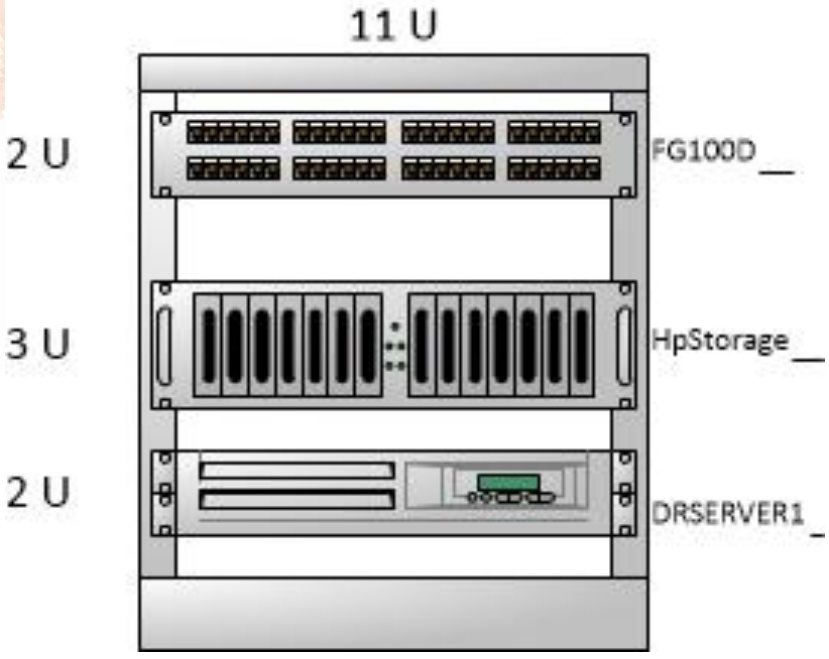
PDC Structure



CBS Failover



DRC Structure



11. Rehearsal, Maintain and Review

It is critical task to plan and perform the rehearsal for the use of Business Continuity and Disaster Recovery. This may be done as part of a training/exercise and is a key factor for the successful implementation of the plan during the crisis. BCP Committee ensures that testing is regular and updated.

After each crisis management, it needs to review the performance of the plan, highlighting how the issue was tackled and what found short on the plan. Crisis management structure may require changes. All kinds of review and changes have to be recorded with the information of review date, reason for review and changes made.

Basic objectives of the testing will be:

- to check that the crisis management mechanism are intact
- to check that all parties have sufficient knowledge of the plan and plan is adequately documented
- to check that proposed plans/actions are achievable
- to check business continuity
- to check that set strategies, technology are up to date
- to generate confidence in the business continuity plan

Bank shall maintain below information as an integral part of the framework. Management update and circulate the information as required in the appendix whenever requires.

a. Employee Telephone Lists
b. Recovery Priorities for Critical Business Functions
c. Alternate Site Recovery Resources Requirements
d. Emergency Operations Centre (EOC) Locations
e. Vital Records
f. Forms and Suppliers
g. Vender Lists
h. Recovery Tasks List

Board of Directors:

S.N.	Name	Position	Signature
1.	Mr. Upendra Keshari Neupane	Chairman	
2.	Mr. Iman Singh Lama	Director	
3.	Mr. Chandra Prasad Bastola	Director	
4.	Mr. Madhav Prasad Bhatta	Director	
5.	Mr. Krishna Shrestha	Director	
6.	Dr. Kailash Patendra Amatya	Director	