Bank Resona Perdania

RESONA

Pedoman *Disaster Recovery Plan*
Sistem *Core Banking*

Disaster Recovery Plan of
Core Banking System Guidelines

Edisi 4, April 2023
4th Edition, April 2023

BOD Approval No. 129/ITD/IT-PLN/V/2023

DAFTAR ISI
Table of Contents

I. PENDAHULUAN

I.1 Latar Belakang

Sistem Core Banking merupakan sistem utama Bank untuk memberikan layanan dan transaksi kepada nasabah. Sistem *Core Banking* memuat informasi penting Bank seperti informasi nasabah, data rekening, data transaksi dan informasi keuangan Bank. Mengingat pentingnya Sistem *Core Banking* bagi kelanjutan operasional Bank, maka Bank harus memastikan Sistem *Core Banking* harus selalu siap untuk digunakan. Oleh karena itu Bank wajib menyiapkan suatu dokumen Rencana Pemulihan Bencana.

I.2 Acuan

1. POJK No. 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum

2. SEOJK No. 21/SEOJK.03/2017 tanggal 6 Juni 2017 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

   SEOJK No. 21/SEOJK.03/2017 ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.11/POJK.03/2022.

3. POJK No.18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum;

   Sejak 30 Oktober 2021,Pasal 20, Pasal 21, Pasal 22, dan Pasal 24 dalam POJK No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum dinyatakan dicabut dan tidak berlaku oleh POJK No.13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum.

4. SEOJK No.34 No.34/SEOJK.03/2016 tanggal 1 September 2016 perihal Penerapan Manajemen Risiko bagi Bank Umum;

I. INTRODUCTION

I.1 Background

The Core Banking System is the Bank's main system for providing services and Bank transactions to customers. The Core Banking System contains Bank important information such as customer information, account data, transaction data and Bank financial information. Considering the importance of the Core Banking System for the continuation of Bank operations, Banks must ensure that the Core Banking System must always be ready for use. Therefore, Banks are required to prepare *Disaster Recovery Plan.*

I.2 Reference

1. POJK No. 11/POJK.03/2022 concerning Application of Information Technology by Commercial Banks

2. SEOJK No.21/SEOJK.03/2017 dated 6 June 2017 concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks.

   SEOJK No. 21/SEOJK.03/2017 is declared to remain valid as long as it does not conflict with the provisions in POJK No.11/POJK.03/2022

3. POJK No.18/POJK.03/2016 concerning Implementation of Risk Management for Commercial Banks;

   Since October 30, 2021, Article 20, Article 21, Article 22 and Article 24 in POJK No.18/POJK.03/2016 concerning Implementation of Risk Management for Commercial Banks has been declared repealed and no longer valid by POJK No.13/POJK.03 / Year 2021 concerning Implementation of Commercial Bank Products.

4. SEOJK No.34/SEOJK.03/2016 dated 1 September 2016 concerning Implementation of Risk Management for Commercial Banks;

5. SEOJK No.29/SEOJK.03/2022 tanggal 27 Desember 2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum.
6. Kebijakan Tingkat Otorisasi.
7. Kebijakan Manajemen Risiko Secara Umum (Individual).
8. Kebijakan Manajemen Risiko Teknologi Informasi.
9. Kebijakan Audit *Intern* Teknologi Informasi.
10. Kebijakan Manajemen Proyek dan Pengembangan Sistem..
11. Kebijakan Manajemen Kelangsungan Usaha.
12. Kebijakan Pengawasan Keamanan Sistem dan Informasi.
13. Kebijakan *Business Continuity Plan* Operasional Sistem.
14. Kebijakan Tugas dan Wewenang.
15. Kebijakan *Job Description*.

I.3 Tujuan

Untuk memberikan panduan kepada pihak-pihak terkait dalam mempersiapkan Sistem *Core Banking* pada unit *on-site backup* (*Standby*) atau unit *off-site backup (DR)* dalam hal unit produksi bermasalah atau tidak dapat di akses oleh pengguna.

I.4 Pihak Terkait

Kepala Divisi TI mengkoordinasikan pelaksanaan Rencana Pemulihan Bencana, dengan tugas dan tanggungjawab sebagai berikut :

1. **Fungsi Operasional dan Dukungan Teknologi :**

   - Memastikan versi *operating* sistem, *database* dan sistem aplikasi yang di*instal* di unit produksi sudah di-*update*

5. SEOJK No.29/SEOJK.03/2022 dated 27 December 2022 concerning Cyber Security and Resilience for Commercial Banks.
6. Levelling of Authority Policy.
7. Individual General Risk Management Policy.
8. Information Technology Risk Management Policy.
9. Information Technology Internal Audit Policy.
10. Project Management and System Development Policy.
11. Business Continuity Management Policy.
12. System and Information Security Monitoring Policy.
13. Business Continuity Plan Policy of Operational System.
14. Duties and Authorities Policy.
15. Job Description Policy.

I.3 Purpose

To provide a guidelines to related parties in preparing Core Banking System at on-site backup (Standby) or off-site backup (DR) units in case production unit has problem or cannot be accessed by the user.

I.4 Related Parties

IT Division Head coordinating Disaster Recovery Plan with the task and responsible as follows :

1. **IT Support and Operational Function :**

   - Ensure operating system, database and application system versions installed in the production unit have ke unit *on-site backup* (*Standby*) dan *off-site backup (DR)units*.

- Melakukan proses *backup* data profil pengguna di unit produksi dan melakukan *restore* di unit *off-site backup (DR)* secara berkala.

- Melakukan proses *backup database* harian pada unit produksi dan memastikan hasil *backup* dapat digunakan. (tidak ada kesalahan saat proses *backup database* di unit produksi dan menyimpan media di lokasi yang aman dan dapat diambil saat akan digunakan).

- Melakukan proses *restore database* secara manual untuk keperluan uji coba/*testing* atau kondisi *disaster*.

- Mengaktifkan *server on-site backup* atau *off-site backup (DR)* yang akan digunakan sebagai pengganti unit produksi

- Memastikan program, *object* dan *patch* yang di*install* di unit produksi sudah *update* ke unit *on-site backup* dan *off-site backup (DR).*

- Memastikan semua *tools* atau program khusus yang digunakan di unit *off-site backup (DR)* sudah di uji coba dan hasilnya sudah benar.

2. Departemen Perencanaan TI :

- Memastikan semua periode *maintenance* untuk infrastruktur di *DRC* sudah diperpanjang sesuai dengan periode.
- Memastikan koneksi jaringan di *DRC* ke *Head Office,* Cabang, dan Cabang Pembantu dan sudah di uji secara berkala.

3. Departemen Sistem TI :

- Memastikan setiap aplikasi yang di kembangkan pada mesin produksi harus di *update* ke mesin DRC

been updated to on-site backup (Standby) and off-site backup (DR) units.

- Conduct back-up of user profile data in the production unit and restore them in the off-site backup (DR) unit periodically.

- Perform daily database backup process at the production unit and ensure the backup results can be used. (no errors during backup process in the production unit and store media in a safe location and can be retrieved when used).

- Perform database restore process manually for the pupose of testing or disaster conditions.

- Enabling on-site backup or off-site backup (DR) server that will be used as production unit replacement

- Ensure programs, objects and patches installed in the production unit have been updated to the on-site backup (Standby) and off-site backup (DR).

- Ensure that all special tools or programs used in the off-site backup (DR) unit have been tested and the results are correct.

2. IT Planning Department :

- Ensure that all infrastructure maintenance periods in the DRC have been properly extended.

- Ensure network connection in DRC to Head Office, Branches, and Sub-Branches and has been tested regularly.

3. IT System Department :

- Ensure that any applications that are enhanced on a production machine must be updated to a DRC engine

4. Fungsi Proyek TI :

- Memastikan untuk aplikasi baru yang ditangani oleh Fungsi Proyek Teknologi Informasi , harus menyiapkan unit DRC jika termasuk kategori kritikal *server*.

I.5 Definisi

1. Rencana Pemulihan Bencana (*DRP*) adalah suatu dokumen berisikan rencana dan tindakan untuk menggantikan dan/atau memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan untuk menanggapi suatu insiden/ permasalahan yang tidak direncanakan, agar Bank tetap dapat menjalankan kegiatan operasional bisnis yang kritikal.

2. Pusat Data (*Data Center*) adalah suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya untuk keperluan penyimpanan, dan pengolahan data.

3. *On-site backup (Standby)* adalah suatu pusat data (*data center*) cadangan yang ditempatkan pada lokasi yang sama dengan unit produksi, yang digunakan untuk memulihkan kembali data dan atau informasi serta fungsi-fungsi elektronik yang terganggu atau rusak akibat terjadinya suatu kejadian yang tidak direncanakan.

4. *Off-site backup (DRC)* adalah suatu pusat data (*data center*) cadangan yang ditempatkan pada lokasi yang terpisah dari lokasi unit produksi, yang digunakan untuk memulihkan kembali data/informasi, fungsi-fungsi penting sistem elektronik yang terganggu atau rusak akibat terjadinya suatu kejadian yang tidak direncanakan.

4. IT Project Function :

- Ensure for new applications handled by IT Project Function, must prepare a DRC unit if it belongs to the category of critical server.

I.5 Definition

1. Disaster Recovery Plan (DRP) is a document which contents of plan and action to replace and/or recover data access, hardware and software required, for responding unplanned incidents/problems, so Bank is still able to carry out critical business operational.

2. Data Center (Data Center) is a facility used to place the electronic system and its related components for the purposes of storing and data processing.

3. On-site backup (Standby) is a data center backup that is placed in the same location as the production unit, which is used to recover data and or information, and electronic functions that are disturbed or damaged due to due to occurrence an unplanned event.

4. Off-site backup (DRC) is a data center backup that placed at a location separate from the location of the production unit, that is used to recover data/ information, important functionalities of electronic system which are disrupted/damaged due to occurrence an unplanned event.

II. KONFIGURASI SISTEM

Saat ini sistem *Core Banking* Bank masih menggunakan metode *warm-backup*, dimana proses *switch* dari unit produksi ke unit *on-site backup/off-site backup* masih dilakukan secara manual. Bank memiliki 3-unit *server* untuk menjaga kelangsungan operasional Bank, yaitu :

a. Unit Produksi
b. Unit *On-site backup (Standby)*
c. Unit *Off-site backup (DRC)*

Selain 3-unit *server* diatas, Bank juga memiliki 2-unit lainnya untuk pengembangan sistem (unit *Development*) dan uji coba (unit TEST).

Berikut ini diagram dari arsitektur sistem *Core Banking* dilokasi Data Center (DC) dan *Disaster Recovery Center* (DRC).

II.1 Diagram CBS

II. SYSTEM CONFIGURATION

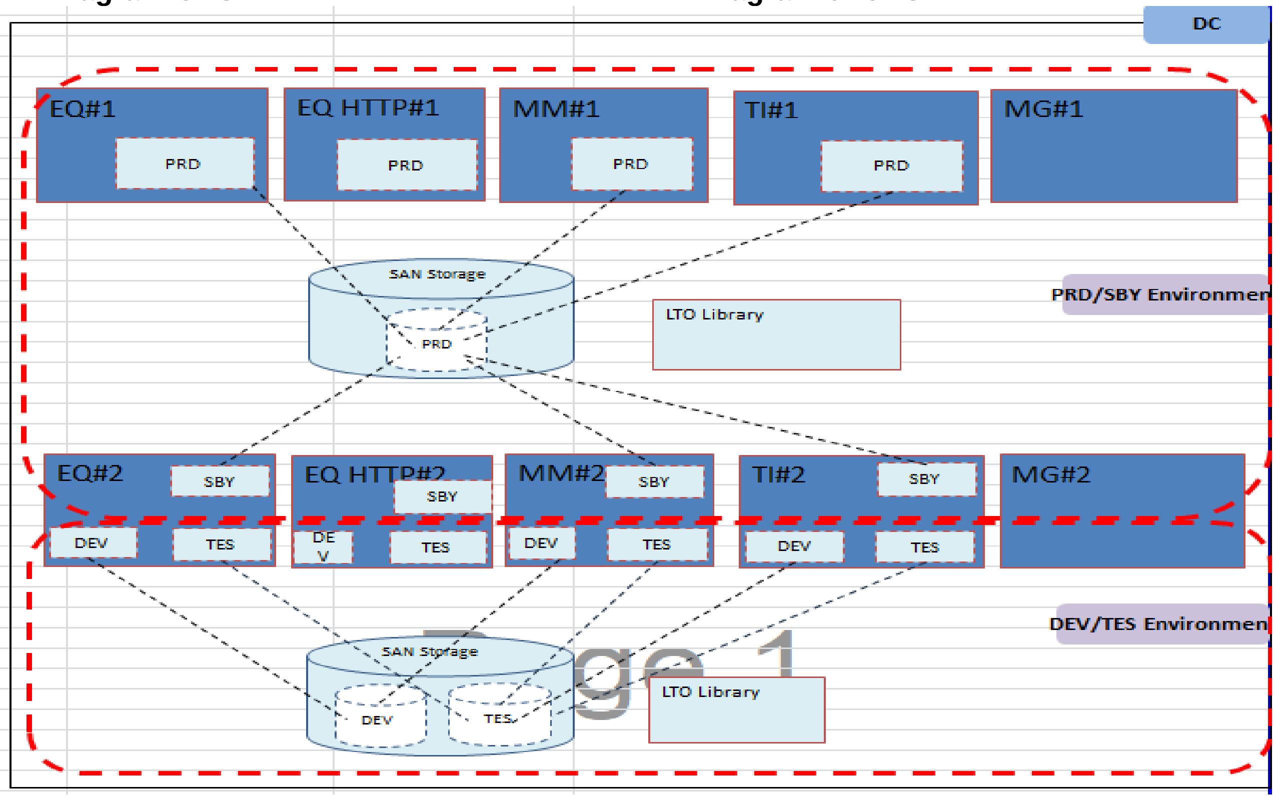
Currently CBS Bank system still uses warm-backup method, where the switch process from production unit to on-site backup / off-site backup unit is still done manually. The bank has 3-unit servers to maintain the continuity of bank operations, namely:

a. Production unit
b. On-site backup (Standby) unit
c. Off-site backup (DRC) unit

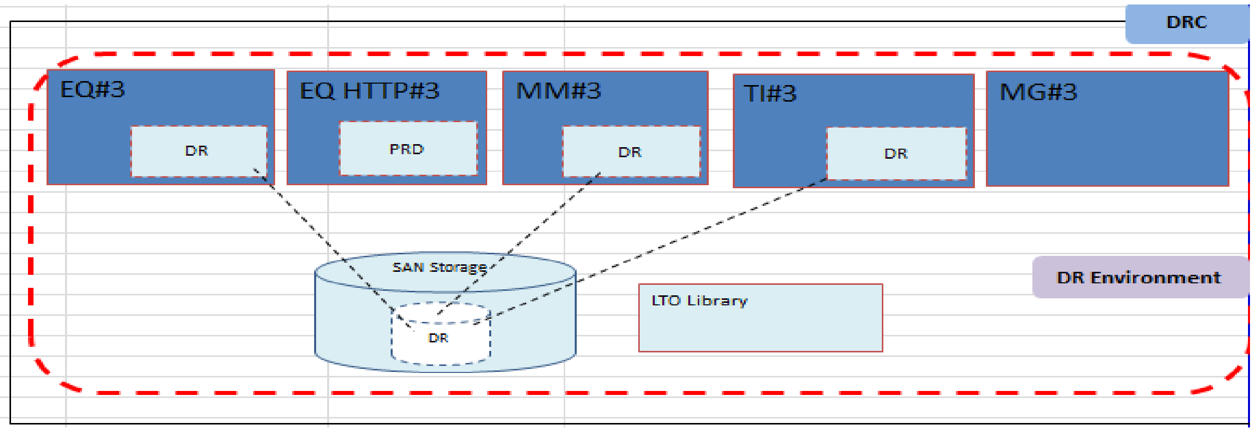
In addition to the 3-units above, bank also has 2 other units for development (Development unit) and testing (Test unit).

Following is diagram of Core Banking system architecture at the Data Center (DC) and Disaster Recover Center (DRC) locations.

II.1 Diagram of CBS



2.1. Gambar Arsitektur Sistem di DC



2.2. Gambar Arsitektur Sistem di DRC

II.2 Perangkat Keras

II.2 Hardwares

No.	Platform/Server	Nama Aplikasi	Serial No.	IP Address	add info	Lokasi
1	Power System S814 (P10)	FBEQ - Production	P6822ADX	192.168.100.12	IP NAT : 10.10.120.2	DC
		UXP Production	010FBEQAP1	192.168.100.13	---	
	IBM P10	FBEQ - Standby	S6822ACX	192.168.100.112	Clustering	DC
		UXP Standby	010FBEQAPS	192.168.100.37		
		FBEQ - Development	D6822ACX	192.168.101.12		
		UXP Development	010FBEQAPD	192.168.101.13		
		FBEQ - testing	T6822ACX	192.168.101.36		
		UXP DRC	010FBEQAPR	192.168.120.43		
	Power System S814 (P10)	FBEQ-DRC	R6822ACX	192.168.120.42	---	DRC
		UXP DRC	010FBEQAPR	192.168.120.43		
2	HP ProLiant DL360 Gen9	FBTI - Production	010FBETI001	192.168.100.26	---	DC
	HP ProLiant DL360 Gen9	FBTI - Standby	010FBTISBY	192.168.100.51	VMWare	DC
		FBTI - Development	010FBTIDEV	192.168.101.27		DC
		FBTI - Testing	010FBTITES	192.168.101.51		DC
	HP ProLiant DL360 Gen9	FBTI - DRC Console	012FBTI001	192.168.120.56	---	DRC
3	HP ProLiant DL360 Gen9	FBMM - Production	010FBMMIN1	192.168.100.23	---	DC
	HP ProLiant DL360 Gen9	FBMM - Standby	010FBMMSBY	192.168.100.46	VMWare	DC
		FBMM - Development	010FBMMDEV	192.168.101.23		DC
		FBMM - Testing	010FBMMTES	192.168.101.46		DC
	HP ProLiant DL360 Gen9	FBMM - DRC	010FBMMEX1	192.168.120.53	---	DRC
4	HP ProLiant DL360 Gen9	HTTP - Production	010FBEQH01	192.168.100.16	---	DC
	HP ProLiant DL360 Gen9	HTTP - Standby	010FBEQSBY	192..168.100.41	VMWare	DC
		HTTP - Development	010FBEQDEV	192.168.101.19		DC
		HTTP - Testing	010FBEQTES	192.168.101.20		DC
	HP ProLiant DL360 Gen9	HTTP - DRC	010FBEQH01	192.168.120.46	---	DRC
5	HP ProLiant DL360 Gen9	NetBackup	010CBSBKP1	192.168.100.31	---	DC
	HP ProLiant DL360 Gen9	NetBackup	010CBSBKPD	192.168.101.31	---	DC
	HP ProLiant DL360 Gen9	NetBackup	012CBSBKP1	192.168.120.61	---	DRC

II.3 Aplikasi

Berikut daftar aplikasi yang diklasifikasikandalam sistem *Core Banking*:

II.3 Application

The following is list of applications that are classified in Core Banking system:

No.	Server Name	Main Application	Describe
1	*EQ Server*	*Fusion Banking Equation* (FBEQ)	*Server* ini memiliki fungsi utama untuk aktifitas dan operasional bank. *This server has the main function for the bank's activities and operations*
2	*EQ HTTP Server*	*Fusion Banking Equation* (HTTP)	*Server* ini berfungsi untuk akses sistem *Core Banking* dalam *web version* (HTTP). Fungsi ini masih dalam pengembangan *This server works for core banking system access in web version (HTTP). This function is in development*
3	*MM server*	*Fusion Banking Message Manager (FBMM)*	*Server* ini berfungsi sebagai perantara sistem *core banking* dengan sistem terkait lainnya. *This server functions as an intermediary of core banking system with other related systems.*
4	*TI Server*	*Fusion Banking Trade Innovation (FBTI)*	*Server* ini digunakan untuk memproses transaksi *Remittance* dan *Trade Finance*. *This server has the function to process Remittance and Trade Finance transactions*
5	*MG Server*	*NetBackup (Middleware for system backup)*	Server ini digunakan untuk pengelolaan *tape backup*. *This server has the function to handle tape backup*

II.4 Jaringan dan Keamanan

Sistem *Core Banking* ditempatkan pada jaringan tersendiri, dimana untuk koneksi sistem *Core Banking* dan sistem Bank lainnya akan melalui *router* yang dipasang dalam jaringan sistem *Core Banking* sebagai titik demarkasi jaringan.

II.4 Network and Security

The Core Banking system is placed on a separate network, where to connect the Core Banking system and other Bank systems through a router that is installed in the Core Banking system network as a network demarcation point.

III. AKTIVASI SISTEM

III.1 Tahap Proses Aktivasi

Proses aktivasi dilakukan untuk keperluan *test*/pelatihan atau dalam kondisi dinyatakan darurat, dimana sistem *Core Banking* produksi bermasalah dan tidak dapat diselesaikan segera. Untuk proses aktivasi akan mengacu pada "KEBIJAKAN *BUSINESS CONTINUITY PLAN OPERASIONAL SISTEM*" Ada 2-kondisi yang dapat dilakukan untuk melakukan proses *recovery*, yaitu melakukan aktivasi pada sistem *Core Banking on-site backup* atau aktivasi sistem *Core Banking off-site backup*.

III.2 Aktivasi *On-site Backup (Standby)*

Proses aktivasi *on-site backup* (*Standby*) dilakukan dalam hal kondisi *Data Center* tetap berfungsi dengan baik, tetapi salah satu *server* yang digunakan sistem *Core Banking* bermasalah. Proses pengaktifan *on-site backup (Standby)* dilakukan dengan mengganti seluruh *server* sistem *Core Banking* dari unit produksi ke unit *Standby*.

III. SYSTEM ACTIVATION

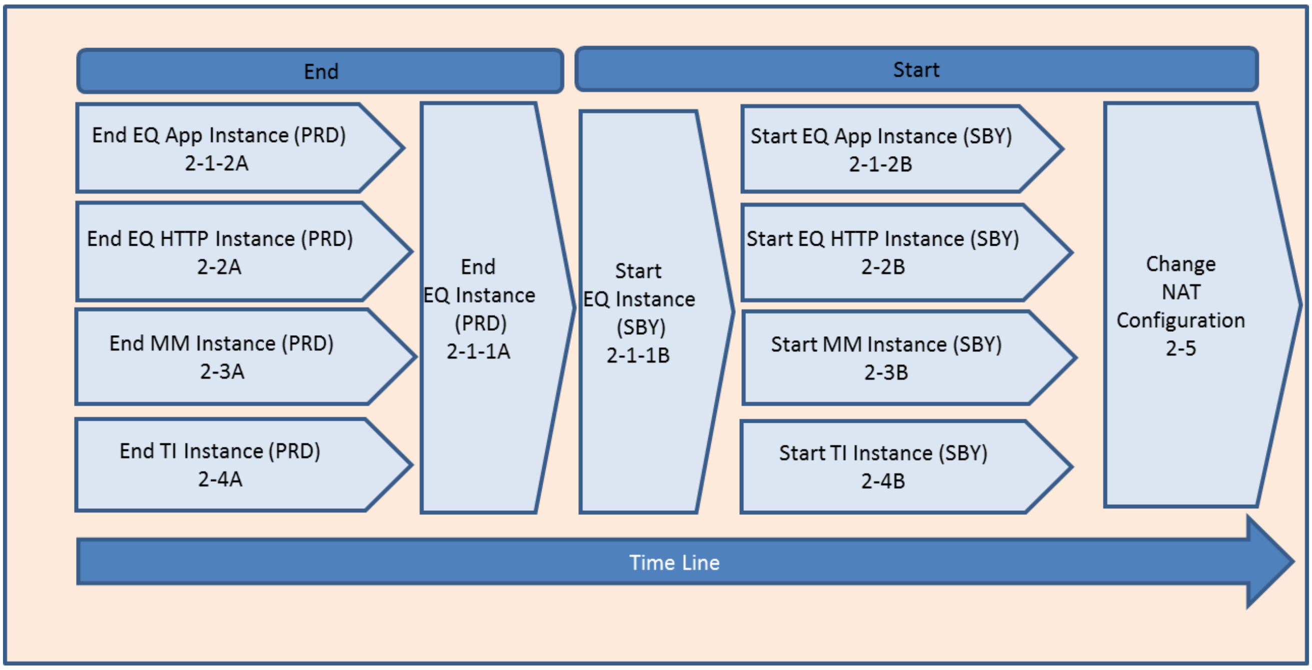
III.1 Activation Stage Process

The activation process is carried out for test /training purposes or in an emergency condition, where Core Banking system production is in trouble and cannot be resolved soon. The activation process will refer to the "BUSINESS CONTINUITY PLAN OPERATIONAL POLICY SYSTEM" There are 2 conditions that can be done to carry out the recovery process, which is to activate the on-site backup Core Banking system or the activation of the off-site backup Core Banking system.

III.2 On-site Backup (Standby) activation

On-site backup (Standby) activation process is carried out in case Data Center is running well but one or more server(s) used by Core Banking system has problem. The activation process of on-site backup (Standby) is done by replacing all Core Banking system servers from the Production unit to Standby unit.

Bagan alur Pemindahan / Switch Over Flow Chart


End
Start
End EQ App Instance (PRD) 2-1-2A
End EQ HTTP Instance (PRD) 2-2A
End MM Instance (PRD) 2-3A
End TI Instance (PRD) 2-4A
End EQ Instance (PRD) 2-1-1A
Start EQ Instance (SBY) 2-1-1B
Start EQ App Instance (SBY) 2-1-2B
Start EQ HTTP Instance (SBY) 2-2B
Start MM Instance (SBY) 2-3B
Start TI Instance (SBY) 2-4B
Change NAT Configuration 2-5
Time Line

1.3 Switch over flowchart

Diagram ini merupakan langkah proses bagaimana cara *Switch Over* dari mesin *Production* ke mesin *Standby*.

1. Mematikan semua *services* di mesin produksi di *EQ app instances*, *EQ HTTP Instances*, *MM Instances* dan *TI Instances* dengan mengacu ke gambar 2-1-2A, 2-2A, 2-3A, 2-4A
2. Mematikan semua *services* and semua varian perangkat IASP yang ada di area *EQ instances production* dengan mengacu pada gambar 2-1-1A
3. Menyalakan semua *services* dan varian perangkat IASP yang ada di EQ *instances Standby* dengan mengacu ke 2-1-1B
4. Menyalakan semua *services* di area *Standby EQ app instances*, *EQ HTTP instances, MM instances* dan *TI instances* dengan mengacu ke 2-1-2B, 2-2B, 2-3B, 2-4B.
5. Mengubah Konfigurasi NAT dari *Environment* ke *Environment Standby* dengan mengacu ke 2-5.

Catatan :
Untuk mengalihkan kembali ke *environment* produksi, bisa mengikuti langkah yang sama, dimana *environment* "*Standby*" yang menjadi bagian untuk di non-aktifkan dan *environment* produksi menjadi *environment* yang harus di aktifkan

Prosedur/Aktifitas untuk mengaktifkan unit *on-site backup (Standby)* adalah sebagai berikut:

<u>Menghentikan Instance Unit Produksi</u> :

A. FBEQ Instance / 2-1-1A

- *Login FBEQ using QSECOFR*
- *Stop [MQRESONA] - Queue Manager*
- *Stop/End [MQRESONA] - Queue Manager*

This flowchart is the step-by-step process on how to conduct Switch Over from Production to Standby.

1. End all services on Production Environment of EQ App Instances, EQ HTTP Instances, MM Instances and TI Instances by referring to 2-1-2A, 2-2A, 2-3A, 2-4A.
2. End all services and vary off IASP devices on EQ Instances Production Environment by referring to 2-1-1A.
3. Start all services and vary on IASP devices on EQ Instances Standby Environment by referring to 2-1-1B.
4. Start all services on Standby Environment of EQ App Instances, EQ HTTP Instances, MM Instances and TI Instances by referring to 2-1-2B, 2-2B, 2-3B, 2-4B.
5. Change the NAT Configuration from Production Environment to Standby Environment by referring to 2-5.

Note :
To switch back again to Production Environment, follow the same step, instead the Standby Environment become the Environment that needed to be End and Production Environment become the Environment that needed to be Start.

The procedure/activities for activating on-site backup unit (Standby) is as follows:

<u>End Instance Production Unit :</u>

A. FBEQ Instance / 2-1-1A

- Login FBEQ using QSECOFR
- Stop [MQRESONA] - Queue Manager
- Stop/End [MQRESONA] - Queue *Manager*

- *End Sub-System [QMQM]*

B. FBEQ App. Instance / 2-1-2A

- *Login SSH with PuTTY*
- *Stop WAS Service*

C. FBEQ HTTP Instance / 2-2A

- *Login/Remote FBEQ HTTP server*
- *Stop Middleware Service EQ HTTP*

D. FBMM Instance / 2-3A

- *Login/Remote FBMM server*
- *Stop Middleware service*
  - *Stop MQ Service*
  - *Stop DB2 Service*

- *Move Share Storage (LUN D) from Production to Standby*
  - *Offline Disk at MM Instance Production VM*
  - *Remove LUN from MM Instance Production VM*
  - *Create Disk at MM Instance Standby VM*

E. FBTI Instance / 2-4A

- *Login/Remote FBTI server*
- *Stop Middleware Services*
  - *Stop WAS Service*
  - *Stop DB2 Service*

Move Share Storage (LUN D) from Production to Standby

<u>Start Instance unit STANDBY :</u>

A. Start FBEQ Instance / 2-1-1B

- *Login sebagai QSECOFR*
- *Vary on IASP Device*
- *Start MQ service*

B. Start FBEQ App. Instance / 2-1-2B

- *Login SSH menggunakan PuTTY*
- *Start WAS service*

- *End Sub-System [QMQM]*

B. FBEQ App. Instance / 2-1-2A

- *Login SSH with PuTTY*
- *Stop WAS Service*

C. FBEQ HTTP Instance / 2-2A

- *Login/Remote FBEQ HTTP server*
- *Stop Middleware Service EQ HTTP*

D. FBMM Instance / 2-3A

- *Login/Remote FBMM server*
- *Stop Middleware Services*
  - *Stop MQ Service*
  - *Stop DB2 Service*

- *Move Share Storage (LUN D) from Production to Standby*
  - *Offline Disk at MM Instance Production VM*
  - *Remove LUN from MM Instance Production VM*
  - *Create Disk at MM Instance Standby VM*

E. FBTI Instance / 2-4A

- *Login/Remote FBTI server*
- *Stop Middleware Services*
  - *Stop WAS Service*
  - *Stop DB2 Service*

- *Move Share Storage (LUN D) from Production to Standby*

<u>Start Instance of STANDBY unit :</u>

A. Start FBEQ Instance / 2-1-1B

- *Login as QSECOFR*
- *Vary on IASP Device*
- *Start MQ service*

B. Start FBEQ App. Instance / 2-1-2B

- *Login SSH using PuTTY*
- *Start WAS service*

C. Start FBEQ HTTP Instance / 2-2B

- *Login/Remote server FBEQ HTTP*
- *Start Middleware service EQ HTTP*

D. Start FBMM Instance / 2-3B

- *Login/Remote FBMM Instance*
- *Start Middleware Services*
    - *Start MQ Service*
    - *Start DB2 Service*
    - *Catalog Database*

E. Start FBTI Instance / 2-4B

- *Login/Remote to FBTI Instance*
- *Start Middleware Services di FBTI Instance*
    - *Online LUN D*
    - *Start WAS Service*
    - *Start DB2 Service*
    - *Catalog Database*

Ubah konfigurasi NAT di *Router sistem Core Banking :*

III. 3 Aktivasi *Off-Site Backup* (DR)

Proses aktivasi *off-site backup (DR)* dilakukan dalam hal kondisi Data Center tidak berfungsi atau tidak dapat diakses karena adanya gangguan ataupun suatu insiden yang tidak direncanakan.

Prosedur/Aktifitas yang perlu dilakukan di *server* DR meliputi :

1. *STOP - FBTI Websphere*
    a. *Login to FBTI WebSphere Admin Console*
    b. *Stop FBTI WebSphere Application*
    c. *Stop WAS Node Agent*
    d. *Stop Deployment Manager*
2. *STOP FBTI services*
    a. *Login/Remote to FBTI Server*
    b. *Stop Equation-TI Integration*

C. Start FBEQ HTTP Instance / 2-2B

- *Login/Remote FBEQ HTTP server*
- *Start Middleware service EQ HTTP*

D. Start FBMM Instance / 2-3B

- *Login/Remote FBMM Instance*
- *Start Middleware Services*
    - *Start MQ Service*
    - *Start DB2 Service*
    - *Catalog Database*

E. Start FBTI Instance / 2-4B

- *Login/Remote to FBTI Instance*
- *Start Middleware Services di FBTI Instance*
    - *Online LUN D*
    - *Start WAS Service*
    - *Start DB2 Service*
    - Catalog Database

Change NAT configuration in router of Core Banking system

III.3 Off-Site Backup (DR) activation

Off-site backup (DR) activation process is carried out in condition that the Data Center is not functioning or cannot be accessed due to an interruption or unplanned incidents.

Procedures/activities that need to be carried out includes:

1. STOP - FBTI Websphere
    a. Login to FBTI WebSphere Admin Console
    b. Stop FBTI WebSphere Application
    c. Stop WAS Node Agent
    d. Stop Deployment Manager
2. STOP FBTI services
    a. Login/Remote to FBTI Server
    b. Stop Equation-TI Integration

3. *STOP FBMM MQ – Channel*
    a. *Login/Remote to FBMM Server*
    b. *Stop MQ Channel – [FBMMQM1.TO.MQRESONA]*

4. *STOP FBEQ – MQ Channel*
    a. *Login to FBEQ server using EQUATION userId*
    b. *Stop MQ Channel – [MQRESONA.TO.FBMMQM1]*

5. *STOP FBMM MQ – Manager*
    a. *Login/Remote to FBMM Server*
    b. *Stop MQ Manager – [FBMMQM1.TO.MQRESONA]*

6. *STOP FBEQ – Jobs and Sub-Systems*
    a. *Login to FBEQ server using EQUATION userId*
    b. *Suspense – FBEQ Application*
    c. *Stop Unit Monitor – EBA Connection*
    d. *d. Stop FBEQ Jobs and Sub Systems (QBATCH/JOBRIM, BAnnnn, EQ3_BAA, PSAKSBS, RTOUTSBSD/RTGS0)*
    e. *e. Stop MMIS (Message Manager Interface for SWIFT) – [EMI – Option]*
    f. *Stop Queue Manager – [MQRESONA]*
    g. *Stop Sub-System – [QMQM]*

7. *UXP – Stop Application*
    a. *Stop UXP/HTTP server*

8. *Restore iSeries User Profiles*
    a. *Login to FBEQ Server using QSECOFR*
    b. *Restore User Profiles (RTSUSRPRF) from last backup (Omit some UserID)*
    c. *Restore Authority (RSTAUT)*
    d. *Start Sub-System–QCTL and Start TCP/IP Server (STRTCPSVR)*

9. *Restore FBEQ system and database library.*

    Ada 5-*library* yang akan perlu di-*restore* (KINPBDP, KFILBDP, KLIBBDP, KWRKBDP dan USRBASELIB)

3. STOP FBMM MQ – Channel
    c. Login/Remote to FBMM Server
    d. Stop MQ Channel – [FBMMQM1.TO.MQRESONA]

4. STOP FBEQ – MQ Channel
    c. Login to FBEQ server using EQUATION userId
    d. Stop MQ Channel – [MQRESONA.TO.FBMMQM1]

5. STOP FBMM MQ – Manager
    c. Login/Remote to FBMM Server
    d. Stop MQ Manager – [FBMMQM1.TO.MQRESONA]

6. STOP FBEQ – Jobs and Sub-Systems
    a. Login to FBEQ server using EQUATION userId
    b. Suspense – FBEQ Application
    c. Stop Unit Monitor – EBA Connection
    d. Stop FBEQ Jobs and Sub-Systems (QBATCH/JOBRIM, BAnnnn, EQ3_BAA, PSAKSBS, RTOUTSBSD/RTGS0)
    e. Stop MMIS (Message Manager Interface for SWIFT) – [EMI – Option]
    f. Stop Queue Manager – [MQRESONA]
    g. Stop Sub-System – [QMQM]

7. UXP – Stop Application
    b. Stop UXP/HTTP server

8. Restore iSeries User Profiles
    e. Login to FBEQ Server using QSECOFR
    f. Restore User Profiles (RTSUSRPRF) from last backup (Omit some UserID)
    g. Restore Authority (RSTAUT)
    h. Start Sub-System–QCTL and Start TCP/IP Server (STRTCPSVR)

9. Restore FBEQ system and database library.

    Ada 5-library yang akan perlu di-restore (KINPBDP, KFILBDP, KLIBBDP, KWRKBDP dan USRBASELIB)

10. Restore FBTI database
FBTI Global database, FBTI Zone database, FBTI MCH database, DB2 Roll forward, Re-config FBTI Deployment address.

11. Restore FBMM database
FBMM database, DB2 Roll forward.

12. Start FBEQ Aplikasi
Call YEMENU; 3-Release Input System

13. Start FBEQ Connection with EBA
STRBA; Call YEMENU; 5-KMENUB; 12-Start Unit Monitor.

14. Start Meridien Replication Sub-System
STRSBS REPEQNBDP

15. Start FBTI Connection
Open service [msc]; Start IBM Websphere; Start [EquationTIIntegration]

16. *Start FBMM application*
Run – [E:\fpm-6.1.x.x.x\bin\Start.bat]

17. Start FBMM [Channel]
Open IBM WebSphere; Start – [Queue Manager; FBMMQM1; FBMMQM1.TO.MQRESONA]

18. Start FBEQ [Channel]
Wrkmqm; 20-MQRESONA; 14-MQRESONA.TO.FBMMQM1

Untuk detil pelaksanaannya, bisa dilihat pada *[WI - DRC Restore & Activation Application* v01.00]

10. Restore FBTI database
FBTI Global database, FBTI Zone database, FBTI MCH database, DB2 Roll forward, Re-config FBTI Deployment address.

11. Restore FBMM database
FBMM database, DB2 Roll forward.

12. Start FBEQ Aplikasi
Call YEMENU; 3-Release Input System

13. Start FBEQ Connection with EBA
STRBA; Call YEMENU; 5-KMENUB; 12-Start Unit Monitor.

14. Start Meridien Replication Sub-System
STRSBS REPEQNBDP

15. Start FBTI Connection
Open service [msc]; Start IBM Websphere; Start [EquationTIIntegration]

16. Start FBMM application
Run – [E:\fpm-6.1.x.x.x\bin\Start.bat]

17. Start FBMM [Channel]
Open IBM WebSphere; Start – [Queue Manager; FBMMQM1; FBMMQM1.TO.MQRESONA]

18. Start FBEQ [Channel]
Wrkmqm; 20-MQRESONA; 14-MQRESONA.TO.FBMMQM1

For detailed implementation, can be seen in [WI - DRC Restore & Activation Application v01.00]

IV. PEMELIHARAAN ENVIRONMENT DRP

Divisi TI harus memastikan sistem, infrastruktur dan perangkat-perangkat yang diperuntukan untuk keperluan *on-site* dan *off-site backup* dalam kondisi baik dan bisa digunakan sewaktu-waktu. Oleh karena itu Divisi TI perlu melakukan serangkaian pemeliharaan, *monitor* dan pengujian secara rutin atas hal-hal berikut :

IV.1 Melakukan Monitor dan Pemeliharaan Pada Perangkat-perangkat Komputer dan Jaringan Secara Berkala

Perangkat komputer dan jaringan yang disiapkan untuk keperluan *on-site* dan *off-site backup* selalu dalam kondisi "*On*" walau tidak selalu digunakan, sehingga memungkinkan Bank mengetahui adanya kerusakan atau tidak berfungsinya perangkat tersebut. Oleh karena itu Divisi TI dalam hal ini Departemen Perencanaan Teknologi Informasi dan Fungsi Operasional dan Dukungan Teknologi Informasi serta pihak vendor akan senantiasa melakukan *monitor* dan pemeliharaan perangkat tersebut secara berkala agar perangkat-perangkat tersebut siap digunakan sewaktu-waktu.

IV.2 Pemeliharaan Aplikasi dan Konfigurasi

Sistem *Core Banking* senantiasa berkembang dan berubah untuk berbagai keperluan seperti : bug-fixing, pengembangan layanan dan produk baru, perubahan regulasi, perkembangan teknologi, dsb. Sehubungan Bank masih menggunakan "*Warm*" *backup*, maka perubahan pada unit produksi tidak secara otomatis meng-*update* unit *on-site* dan *off site backup*. Untuk meminimalkan risiko dan juga waktu *recovery*, maka versi aplikasi dan konfigurasi pada on-site dan *off-site backup* harus sama dengan unit produksi. Proses pemeliharaan dilakukan dengan selalu melakukan *update* pada unit *on-site* dan *off-site backup* dalam hal ada perubahan pada unit produksi dan juga bisa melakukan *restore* aplikasi dari unit produksi ke unit *on-site* dan *off-site backup* secara berkala

IV. MAINTENANCE DRP ENVIRONMENT

IT Division must ensure that the systems, infrastructure and devices which intended for on-site and off-site backup are in good condition and can be used at any time. Therefore the IT Division needs to carry out a series of routine maintenance, monitoring and testing of the following:

IV.1 Monitor and Maintain of Computer and Network Devies Regularly.

Computer and network equipments that are prepared for on-site and off-site backup purposes are always in the "On" condition, although not always in use, thus allowing bank know of any damage or the devices are not functioning. Therefore, the IT Division in this case the Information Technology Planning Department and IT Support and Operational Function and the vendor will always monitor and maintain the device regularly so that the devices are ready for use at any time.

IV.2 Application Maintenance and Configuration

The Core Banking system is continuously developing and changing for various purposes such as: bug-fixing, development of new services and products, changing regulations, technological developments, etc. Since the Bank still uses "Warm" backup, changes to the production unit do not automatically update the on-site and off-site backup units. To minimize risk and recovery time, the application version and the configuration at on-site and off-site backup must be the same as production unit. The maintenance process is carried out by always updating on-site and off-site backup units in case there were changes in the production unit and also being able to restore applications from the production unit to the on-site and off-site backup units periodically.

IV.3 Pemeliharaan Data Pengguna

Sistem *Core Banking* ada yang menggunakan *active-directory*, disimpan pada *database* masing-masing aplikasi dan pada level *operating* sistem. Untuk sistem yang menggunakan *active-directory*, tidak ada kendala karena *active-directory* akan selalu sama dengan yang digunakan unit produksi. Demikian pula sistem yang daftar usernya disimpan pada database, karena akan menggunakan data backup terakhir saat akan digunakan. Dalam hal daftar pengguna disimpan pada level operating sistem dan tidak bisa menggunakan active-directory, maka Bank harus senantiasa meng-update daftar penggunanya agar tidak ada perbedaan yang signifikan dengan kondisi terakhir pada unit produksi. Berikut tabel pengguna sistem Core Banking yang perlu di update :

IV.3 Maintain Users Data

There are Core Banking system that use active-directory, stored in its application database and at operating system level. For systems that use active-directory, there are no problems/issues because the active-directory always be updated and will be same with production unit. Likewise, the system whose user list is stored in the database, because it will use last data backup when it will be used. In the condition that user list is stored at operating system level and cannot use active-directory, bank must always update its user list so that there are no significant differences with last conditions in the production unit. The following is table of Core Banking system users that need to be updated :

No	System Name	OS Level	Apps Level	Active Directory	How To Update
1	*FBEQ - Fusion Banking Equation*	Yes	Yes	Yes	- Restore FBEQ-DB - Restore IBM Iseries User Profiles
2	*FBTI - Fusion Banking Trade Innovation*	---	Yes	---	- Restore FBEQ-DB
3	*FBMM - Fusion Banking Message Manager*	---	Yes	Yes	- Restore FBMM-DB
4	*EQ-HTTP - FBEQ HTTP*	---	---	---	---
5	*MG - Middleware for System Backup*	---	---	---	---

IV.4 Pengujian Rencana Pemulihan Bencana

Pengujian Rencana Pemulihan Bencana diperlukan untuk meyakini bahwa Rencana Pemulihan Bencana dapat diimplementasikan dengan baik pada saat terjadi gangguan dan atau bencana. Dimana terdapat ketentuan yaitu :

a. Dilakukan pengujian dan pengkinian secara berkala atas Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

b. Rencana Pemulihan Bencana dan hasil pengujian Rencana Pemulihan Bencana harus dikaji ulang secara berkala, paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

IV.4 Testing of Disaster Recovery Plan

Organization or team work is needed to believe that a disaster recovery plan could be implemented properly when there are a distraction and or disaster. There are the following condition :

a. Will do the test and the updating periodically for Disaster Recovery Plan at least once in 1st (one) year.

b. Disaster Recovery Plan and the result of the testing have to be reviewed periodically, at least 1st (once) in 1st (one) year.

c. Terkait Pengujian Rencana Pemulihan Bencana, uji coba dilakukan atas Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun untuk seluruh sistem atau aplikasi kritikal sesuai hasil analisis dampak bisnis *(Business Impact Analysis)* dan mewakili seluruh infrastruktur yang kritikal serta melibatkan pengguna TI.

d. Dalam hal Bank melakukan perubahan yang sangat mendasar terhadap system, aplikasi, atau infrastruktur TI Bank (misalnya perubahan pada Core Banking System) maka harus dilakukan pengujian Rencana Pemulihan Bencana paling lama 6 (enam) bulan setelah perubahan system dimaksud diimplementasikan.

e. Pengujian yang dilakukan harus didokumentasikan secara tertib dan dievaluasi untuk meyakini efektifitas dan keberhasilan pengujian.

f. Hasil pengujian dan analisis dari setiap permasalahan yang ditemukan pada saat pengujian harus dilaporkan kepada Direksi. Hal yang dilaporkan meliputi:

1. Penilaian ketercapaian tujuan pengujian;
2. Penilaian atas validitas pengujian pemrosesan data;
3. Tindakan korektif untuk mengatasi permasalahan yang terjadi;
4. Deskripsi mengenai kesenjangan antara Rencana Pemulihan Bencana dan hasil pengujian serta usulan perubahannya;
5. Rekomendasi untuk pengujian selanjutnya.

Dalam hal hasil uji coba mengalami kegagalan maka Bank harus mengkaji penyebab kegagalan atau permasalahan yang terjadi dan melakukan pengujian ulang.

c. About Disaster Recovery Plan test, this test will do at least 1st (once) in a year for all of the system or critical application based on Business Impact Analysis result and representing all of the critical infrastructure and involving all of IT user.

d. In case Bank doing some changes which that's very basic against the system, application, or IT Infrastructure of Bank (Example the changes of Core Banking System) so must be do the disaster recovery plan test approximately 6th (six) month after the system changes was implemented.

e. The testing have to be documented in an orderly manner and evaluated to make sure the effectivity and successful testing.

f. The result of testing and analysis from every mistaken that founded on the test must be reporting with the directors. The things that have to be reported are:

1. Evaluation of successfully testing;
2. Evaluation of validity processing data testing;
3. The act of corrective to solve the problem happen;
4. Description of GAP between Disaster Recovery Plan and the result of testing with the proposal of amendment;
5. Recommendation for the next testing.

In the event that the result of the test is failed so Bank have to check the problem that already happen and doing the re-test again.

V. PENUTUP

Dalam hal terjadi gangguan atau kegagalan system *Core Banking* baik *production* ataupun *backup*, maka pedoman ini bisa menjadi acuan dalam proses pengalihan operasional *Core Banking system* dari *Data Center* ke *Disaster Recovery Center (DRC).*

Pedoman ini diterbitkan dalam 2 (dua) bahasa yaitu Bahasa Indonesia dan Bahasa Inggris, dan bilamana terjadi perbedaan penafsiran antara keduanya maka yang menjadi acuan adalah Bahasa Indonesia.

Pedoman ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur tanggal 29 Mei 2023 serta mencabut Pedoman Disaster Recovery Plan Sistem Core Banking Edisi 3, Mei 2022

Pedoman ini akan dikaji ulang secara berkala paling lambat setiap 1 (satu) tahun sekali atau jika diperlukan sebagai upaya penyempurnaan sesuai dengan perkembangan usaha dan kebutuhan Bank atau perubahan peraturan yang mendasarinya.

V. CLOSING

In case there is disorder or failure of both production and backup of Core Banking System, this Guidelines can be also used as reference in Diversion of usage from DC to DRC.

This Guidelines issued in 2nd (two) languages is a Indonesia languages and English languages, and if any dispute or contradiction of them, we should refer to Indonesian version.

These guidelines take effect as approved the President Directors on May 29, 2023 and revoke Disaster Recovery Plan of Core Banking System Guidelines 3rd Edition, May 2022.

This policy will be reviewed at least every 1st (one) years or if needed as an improvement effort following the business development and the need of Bank or following the changes of base regulation.