Bank Resona Perdania

KEBIJAKAN *BUSINESS CONTINUITY PLAN* OPERASIONAL SISTEM
BUSINESS CONTINUITY PLAN POLICY OF OPERATIONAL SYSTEM

Edisi ke-10, April 2023

10th Edition, April 2023

BOD Approval No. 158/ITD/IT-PLN/VI/2023

BOC Approval No.104/BOC/VII/2023-ITD/IT-PLN

DAFTAR ISI
Table of Content

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

Kebutuhan Bank untuk menjamin kegiatan operasional Bank tetap dapat berfungsi walaupun terdapat gangguan atau bencana guna melindungi kepentingan para pemangku kepentingan. Rencana Pemulihan Bencana menekankan pada aspek teknologi dengan fokus pada pemulihan data (*data recovery* atau *restoration plan*) dan berfungsinya sistem aplikasi yang kritikal dan infrastruktur TI yang kritikal dalam waktu dan level operasional yang dapat diterima.

B. 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 Okt 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/SEOJK.03/2016 tanggal 1 September 2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum.

5. PADG No. 23/19/PADG/2021 tanggal 13 September 2021 tentang Penyelenggaraan Aplikasi Layanan

I. INTRODUCTION

A. Background

Bank needs to ensure operational activity is functioned even though there is a disruption or disaster to protect stakeholder's interest. Disaster Recovery Plan emphasizes.in technology aspect by focusing in data recovery or restoration plan) and the functioning of critical application system and critical IT infrastructure in tolerable time and operational level.

B. Reference

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

2. SEOJK No. 21 /SEOJK.03/2017 on June 6th 2017 about Implementation of Risk Management in the use of Information Technology by Public Bank.

   SEOJK No.21/SEOJK.03/2017 is still 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 30 Oct 2021, Article 20, Pasal 21, Article 22, and Article 24 in POJK No. 18/POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks was declared revoked and invalid by POJK No.13/POJK.03/2021 concerning the Operation of Commercial Bank Products.

4. SEOJK No. 34/SEOJK.03/2016 dated 1 September 2016 about Management for Public Bank.

5. PADG No. 23/19/PADG/2021 dated September 13, 2021 concerning Implementation of Bank Indonesia

Bank Indonesia.

Pada saat PADG ini mulai berlaku, SEBI No. 18/2/DPTP tanggal 28 Januari 2016 perihal Penyelenggaraan Sistem BI *Government Electronic Banking* dicabut dan dinyatakan tidak berlaku.

6. Kebijakan Tingkat Otorisasi.
7. Kebijakan Manajemen Risiko secara Umum (Individual)
8. Kebijakan Manajemen Risiko Teknologi Informasi.
9. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi.
10. Kebijakan Manajemen Kelangsungan Usaha.
11. Kebijakan Tugas & Wewenang.
12. Kebijakan Job Description.
13. Kebijakan Audit Intern Teknologi Informasi.
14. Pedoman Rencana Tanggap Darurat.

C. Tujuan

1. Untuk menentukan prioritas fungsi bisnis kritikal.
2. Untuk menganalisa risiko bisnis dalam keadaan darurat.
3. Untuk meminimalkan risiko dengan mendefinisikan detail dari respon dalam keadaan darurat.
4. Untuk memastikan sistem pemulihan yang tepat melalui prosedur yang efektif.

D. Ruang Lingkup

1. Kantor Pusat Bank Resona Perdania dan
2. *Disaster Recovery Center*, jika Kantor Pusat dan/atau *Data Center* tidak

Service Applications.

At the time this PADG comes into force, SEBI No. 18/2/DPTP dated January 28, 2016 regarding the Operation of the BI Government Electronic Banking System is revoked and declared invalid.

6. Levelling of Authority Policy.
7. Individual General Risk Management Policy.
8. Information Technology Risk Management Policy.
9. Information Security and System Risk Management Policy in the use of Information Technology.
10. Business Continuity Management Policy.
11. Duties & Authorities Policy.
12. Job Description Policy.
13. Information Technology Internal Audit Policy.
14. Emergency Response Plan Guideline.

C. Purpose

1. To determine priority of critical business function.
2. To analyze business risk in emergency.
3. To minimize risk by defined detail of response in disaster.
4. To ensure an accurate recovery process by an effective procedure.

D. Scope

1. Head Office Bank Resona Perdania
2. Disaster Recovery Center, if Head Office and/or Data Center is

dapat diakses.

a. Biznet Technovillage Jl. Biznet Technovillage No. 1, Cimanggis Bojong Nangka, Gn. Putri, Bogor, Jawa Barat 16965

b. Cabang Pembantu Cibitung (MM2100) BeFa Square Unit G-B Lantai G, Kawasan Industri MM2100, Cikarang Barat, Bekasi 17842, Jawa Barat, Indonesia

c. Cabang Pembantu Deltamas Kompleks Ruko Palais de Paris Blok D No.10 Perumahan Kota Deltamas, Cikarang Pusat Jawa Barat - Indonesia, Bekasi 17530

E. Asumsi

BCP dirancang berdasarkan asumsi dalam keadaan paling buruk seperti dibawah ini:

1. Skenario terburuk sehubungan dengan bencana alam, gedung tidak dapat diakses atau gedung hancur. Hal tersebut akan memerlukan waktu dalam pemulihan dan perbaikan peralatan.

2. Skenario terburuk terkait *backup* aplikasi *Core Banking* dan aplikasi lainnya dilakukan setelah semua proses operasi selesai (*end of day*). *Tape backup* dikirim ke lokasi penyimpanan *offsite* setiap hari. Apabila terjadi gangguan atau bencana sebelum *backup* dilakukan, maka semua transaksi yang sudah diproses akan hilang.

3. Tempat penyimpanan *backup offsite* berada di lokasi yang aman, cukup dekat untuk dapat diakses dengan mudah dan cepat, dan tidak terpengaruh oleh bencana alam.

F. Istilah dan Definisi

1. Pusat Data (*Data Center*) adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan dan

inaccessible.

a. Biznet Technovillage Jl. Biznet Technovillage No. , Cimanggis Bojong Nangka, Gn. Putri Bogor, Jawa Barat 16965

b. Cabang Pembantu Cibitung (MM2100) BeFa Square Unit G-B Lantai G, Kawasan Industri MM2100, Cikarang Barat, Bekasi 17842, Jawa Barat, Indonesia

c. Cabang Pembantu Deltamas Kompleks Ruko Palais de Paris Blok D No.10 Perumahan Kota Deltamas, Cikarang Pusat Jawa Barat - Indonesia, Bekasi 17530

E. Assumption

BCP is designed base on assumption in disaster such as following:

1. Scenario related to nature disaster, building is inaccessible or building is destroyed. That kind of disaster requires time to recover and repair equipment.

2. Worst scenario related to backup application of core banking and other application done after end of day. Backup tape is send to offsite storage every day. If happen disturbance or disaster before backup is done, all processed transaction will be lost.

3. Secure backup offsite should be easy to access and not impacted from disaster.

F. Term and Definition

1. Data Center is a facility to place electronic system and its related component for data deployment, storage and processing.

pengolahan data.

2. Pusat Pemulihan Bencana (*Disaster Recovery Center*) adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting sistem elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia.

2. Disaster Recovery Center is facility to recover data or information include important functions of disturbed/damaged electronic system caused by disaster or human.

3. Pangkalan Data (*Database*) adalah sekumpulan data komprehensif dan disusun secara sistematis, dapat diakses oleh pengguna sesuai wewenang masing-masing dan dikelola oleh administrator Pangkalan Data (*database administrator*).

3. Database is collective of comprehensive data and systematic, can be access by user according to authority and maintain by database administrator.

4. Rencana Pemulihan Bencana (*Disaster Recovery Plan*) adalah dokumen yang berisikan rencana dan langkah-langkah untuk menggantikan dan/atau memulikan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar Bank dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana.

4. Disaster Recovery Plan is document contain plan and steps to restore and/or recover access data, hardware and software needed so Bank can continue critical business operational after disturbance and/or disaster.

II. TUGAS DAN TANGGUNG JAWAB

A. Direksi

1. Untuk menyetujui Kebijakan, Prosedur dan strategi BCP.
2. Menetapkan BCP yang dikinikan secara berkala.
3. Memastikan adanya tim BCP, yang terdiri dari personil yang kompeten dan terlatih.
4. Meyakini bahwa BCP disosialisasikan kepada seluruh fungsi bisnis dan personil.
5. Pembuat keputusan berhubungan dengan BCP.
6. Sebagai penanggung jawab untuk mengaktifkan BCP ketika terjadi gangguan/bencana.
7. Menginstruksikan pelatihan alur komunikasi.
8. Mengevaluasi hasil pengujian BCP.
9. Mengevaluasi hasil pemeriksaan Audit Internal atas kecukupan BCP.

B. Tim BCM (*Business Continuity Management)*

1. Bertanggung jawab penuh terhadap efektivitas penyelenggaraan BCP.
2. Bertanggung jawab untuk memastikan/melakukan program *awareness* mengenai BCP.
3. Bertanggung jawab melakukan sosialisasi terkait BCP.

II. JOB AND RESPONSIBILITY

A. Board of Directors

1. Approve Policy, Procedure and BCP strategic.
2. Approve BCP that is updated on regular basis.
3. Ensure BCP team is formed from competent and trained personnel.
4. Ensure that BCP is socialized to all business function and personnel.
5. Decision maker about BCP.
6. Responsible to activate BCP during disturbance/disaster.
7. Instruct communication tree training.
8. Evaluate result of BCP
9. Evaluate result of Internal Audit related to BCP adequacy.

B. BCM Team (Business Continuity Management)

1. Responsible to effectiveness of BCP implementation.
2. Responsible to ensure/conduct program awareness about BCP.
3. Responsible in socialization related to BCP.

C. Departemen Perencanaan TI dan Fungsi Operasional dan Dukungan TI

1. Bertanggung jawab untuk melakukan pengujian BCP terhadap sistem kritikal Bank dan membuat laporan hasil pengujian ke Direksi.
2. Bertanggung jawab untuk menentukan skenario pemulihan sistem yang akan digunakan berdasarkan persetujuan *Direktur in Charge*.
3. Bertanggung jawab untuk melakukan pengkinian Kebijakan BCP Sistem Operasional sesuai dengan perkembangan bisnis Bank.
4. Bertanggung jawab untuk melakukan pengkinian *Vendor List* Teknologi Informasi/Sistem jika terdapat perubahan *Person in Charge* di vendor terkait.
5. Bertanggung jawab terhadap efektivitas penyelenggaraan DRC.
6. Melaksanakan komunikasi terhadap pihak internal dan eksternal Bank bila terjadi suatu gangguan yang mengakibatkan terhentinya sistem dan infrastruktur yang kritikal.
7. Bertanggung jawab untuk melakukan pengkinian data terkait sistem aplikasi dan infrastruktur TI di lokasi *Disaster Recovery*.

D. Departemen Sistem TI dan Fungsi Proyek TI

Melakukan koordinasi dengan Departemen Perencanaan TI dan Fungsi Operasional dan Dukungan TI dalam pelaksanaan ujicoba Rencana Pemulihan Bencana.

E. Departemen Pengawas Keamanan Informasi dan Risiko Sistem

1. Bertangggung jawab dalam melakukan pemeliharaan dan pengkinian BIA.

C. IT Planning and Infrastructure and IT Support and Operational Function

1. Responsible to test BCP towards Bank critical system and create report of testing result to Board of Directors.
2. Responsible to determine system recovery scenario to be used, based on approval from Director in Charge.
3. Responsible to update BCP Policy of System Operational according to the development of Bank business.
4. Responsible to update vendor list of Information Technology/System if there is any replacement of Person in Charge.
5. Responsible to effectiveness of DRC implementation.
6. Conduct communication to internal and external Bank if occurs disturbance that result in critical system and infrastructure is down.
7. Responsible to update data related application system and IT infrastructure at Disaster Recovery site.

D. IT System Department and IT Project Function

Coordinate with the IT Planning Department and the IT Operations and Support function in the implementation of the Disaster Recovery Plan pilot.

E. Information Security and System Risk Controller Department

1. Responsible in maintain and update BIA.

F. Departemen Umum

1. Bertanggung jawab untuk melakukan *emergency drill* secara rutin.
2. Bertanggung jawab untuk memastikan bahwa peralatan yang dibutuhkan tersedia ketika dalam keadaan darurat.

G. Departemen/Divisi/Cabang

1. Kepala Departemen/Divisi/Cabang bertugas sebagai Koordinator Tim Pemulihan Usaha pada masing-masing Departemen/Divisi/Cabang ketika terjadi gangguan/keadaan darurat.
2. Kepala Departemen/Divisi/Cabang bertanggung jawab untuk menentukan personil dan melakukan pengkinian Tim Pemulihan Usaha pada masing-masing Departemen/Divisi/Cabang.
3. Kepala Departemen/Divisi/Cabang bertanggung jawab untuk mengupdate alur komunikasi pada masing-masing Departemen/Divisi/Cabang.
4. Bertanggung jawab untuk mengamankan personil Bank dan aset perusahaan ketika dalam keadaan darurat berdasarkan tugas yang telah ditetapkan.
5. Memastikan bahwa masing-masing personil yang ditunjuk oleh Kepala Departemen/Divisi/Cabang sebagai Tim Pemulihan Usaha mengetahui tugas dan tanggung jawabnya.
6. Bertanggung jawab untuk memastikan pengamanan dokumen dan aset pada masing-masing Departemen/Divisi/Cabang dilakukan.

F. General Affair Department

1. Responsible to conduct emergency drill on regular basis.
2. Responsible to ensure that equipment is available in disturbance.

G. Department/Division/Branch

1. Head of Department/Division/Branch responsible as Coordinator of Business Recovery Team in each Department/Division/Branch during disturbance/disaster.
2. Head of Department/Division/Branch responsible to assign personnel and update Business Recovery Team in each Department/Division/Branch.
3. Head of Department/Division/Branch responsible to update communication tree in each Department/Division/Branch.
4. Responsible to secure Bank personnel and company asset during disaster, based on responsibility.
5. Ensure that each personnel that assigned as Business Recovery Team by Head of Department/Division/Branch knows job and responsibility.
6. Responsible to ensure document security and asset at each Department/Division/Branch.

III. BUSINESS IMPACT ANALYSIS

A. *Business Impact Analysis*

Business Impact Analysis, selanjutnya disebut sebagai “BIA” adalah proses untuk menentukan dampak operasional dan finansial Bank apabila proses bisnis dan *Data Center* tidak tersedia dalam waktu tertentu. Tujuan BIA adalah untuk menyediakan analisa dengan mendokumentasikan waktu pemulihan yang dibutuhkan dan dampak finansial yang berhubungan dengan proses kritikal.

B. Dasar Penyusunan BIA

1. Tingkat kepentingan (*criticality*) masing-masing proses bisnis dan ketergantungan antar proses bisnis serta prioritasi yang diperlukan.
2. Tingkat ketergantungan terhadap pihak penyedia jasa, baik TI maupun *non* TI.
3. Tingkat *Maximum Tolerable Outage/ Recovery Time Objective* (berapa lama Bank dapat bekerja tanpa sistem atau fasilitas yang mengalami gangguan dan/ atau berapa cepat sistem atau fasilitas tersebut harus berfungsi kembali).
4. Tingkat *Minimum Resources Requirement* (personil, data dan kelengkapan sistem serta fasilitas yang diperlukan secara minimal agar bisnis bisa pulih dan berjalan).
5. Dampak potensial dari kejadian yang bersifat tidak spesifik dan tidak dapat dikontrol terhadap proses bisnis dan pelayanan kepada nasabah.
6. Dampak *disaster* terhadap seluruh Divisi dan fungsi bisnis, bukan hanya terhadap *data processing*.
7. Estimasi *downtime* maksimum yang dapat ditoleransi dan tingkat toleransi atas kehilangan data dan terhentinya proses bisnis serta dampak *downtime* terhadap kerugian finansial.
8. Jalur komunikasi yang dibutuhkan untuk berjalannya pemulihan.

III. BUSINESS IMPACT ANALYSIS

A. Business Impact Analysis

Business Impact Analysis, hereinafter refer as "BIA" is process to define operational impact and impact to Bank financial if business process and data center is unavailable in a certain time. The purpose of BIA is to provide analysis by documented recovery time needed and financial impact of critical process.

B. Basic of Creating BIA

1. Critical level each business process and dependency among business process include priority.
2. Dependency level to service providers, either TI or non TI.
3. Maximum Tolerable Outage/ Recovery Time Objective level (how long Bank can operate without system or disturbed facility and/or how fast can the system or facility recover.
4. Minimum Resource Requirement level (minimum personnel, data and system adequacy include facility needed so business can recover and operates).
5. Potential impact of event that is not specific and cannot be controlled towards business process and service to customer.
6. Effect of disaster on all Division and business function, not only on data processing.
7. Maximum tolerable downtime estimation and its tolerance level of data loss and downtime impact on financial loss.
8. Communication network required for the recovery process.

9. Kemampuan dan pengetahuan petugas mengenai *Contingency Plan* dan ketersediaan petugas pengganti di tempat pemulihan.

10. Dampak hukum dan pemenuhan ketentuan yang terkait, seperti ketentuan mengenai kerahasiaan data nasabah.

C. Tingkat Kepentingan

Disusun berdasarkan tingkat kepentingan aplikasi yang digunakan dalam proses operasional/bisnis dan ketergantungan antar proses. Mengacu pada Lampiran 1 – *Business Impact Analysis* (BIA).

D. Tingkat *Maximum Tolerable Outage*/*Recovery Time Objective*

Recovery Time Objective, selanjutnya disebut sebagai “RTO” harus terdiri atas

1. Waktu sebelum kondisi darurat diumumkan.

2. Waktu yang dibutuhkan untuk mengaktifkan BCP.

3. Waktu yang dibutuhkan Divisi Teknologi Informasi untuk memulihkan sistem.

4. Waktu yang dibutuhkan Divisi yang terkena dampak untuk mengembalikan keadaan termasuk waktu yang dibutuhkan untuk verifikasi bahwa proses pemulihan komputer telah sesuai dan sinkron.

5. Waktu untuk setiap operasional untuk menyelesaikan transaksi yang belum diproses dan memulihkan ke kondisi semula.

Mengacu pada Lampiran 1 – *Business Impact Analysis* (BIA).

9. Ability and knowledge of officer regarding Contingency Plan and the availability of the substitute officer in recovery site.

10. Legal impact and fulfillment of relevant provision regarding confidentiality of customer's data.

C. Importance Level

Base on application importance level that is use in business/operational process and its dependency between processes. Refer to Annex 1 - Business Impact Analysis (BIA).

D. Level of Maximum Tolerable Outage/Recovery Time Objective

Recovery Time Objective, hereinafter refer as "RTO" consisting of the following

1. Time before emergency condition is announced.

2. Required time to activate BCP.

3. Time for Information Technology Division to recover system.

4. Time for each Division to recover include time to verify that recovery process is done and synced.

5. Time for operational to finish transaction and recover to normal condition.

Refer to Annex 1 - Business Impact Analysis (BIA).

E. *Minimum Resource Requirement*

Minimum Resource Requirement adalah persyaratan minimal yang diperlukan untuk proses pemulihan dan menjalankan aktivitas bisnis. Persyaratan minimal adalah sebagai berikut:

1. Personil
2. Data
3. Kecukupan dan fasilitas sistem

Mengacu pada Lampiran 1 – *Business Impact Analysis* (BIA)

F. Analisa Potensial Dampak dari Gangguan/Bencana

Analisa potensial dampak gangguan/bencana berhubungan dengan sebagai berikut:

1. Dampak operasional mungkin berdampak ke nasabah dan Bank.
2. Dampak finansial, mengacu ke BIA.

Mengacu pada Lampiran 1 – *Business Impact Analysis* (BIA).

G. *Emergency Response*

Hal-hal yang perlu dilakukan Divisi TI dalam hal ada kendala sistem TI adalah sebagai berikut :

1. Divisi TI menerima informasi adanya gangguan/kendala pada sistem TI dari *user* atau anggota Divisi TI.
2. Divisi TI melakukan Identifikasi permasalahan yang terjadi pada sistem seperti : gagal *login*, gagal *input*, gagal proses *approve/release*, sistem *hang*, sistem *off-line* / *error*, *problem interface*, atau lainnya.
3. Jika kendala bisa diselesaikan sebelum batas waktu proses manual, PIC dapat menyelesaikan permasalahan dan selanjutnya melaporkan ke atasan. Jika tidak bisa diselesaikan segera, laporkan ke atasan dan seterusnya sampai ke Direktur In-Charge dalam hal

E. Minimum Resource Requirement

Minimum Resource Requirement is minimum requirement to recovery and to continue business activity. Following is minimum requirement:

1. Personnel
2. Data
3. System adequacy and facility

Refer to Annex 1 - Business Impact Analysis (BIA)

F. Analysis of Potential Impact from Disruption/ Disaster

Potential impact analysis of disruption/disaster related to

1. Operational impact and impact to both customer and Bank.
2. Financial impact, refer to BIA

Refer to Annex 1 - Business Impact Analysis (BIA).

G. Emergency Response

Things that should be taken by IT division in case there was problem are as follows :

1. IT Division received information about any issue/problem in IT system from user dan atau IT division.
2. IT division do identification of problems that happened at system such as : login failed, input failed, process approve/release failed, system hang, system off-line/error, problem interface, or others.
3. If the obstacles can be done before limited time the process manual, PIC can solving the problem and next give report to head. If cant be solve as soon as possible to must be reporting the issue to the head and next reporting to Director in-charge in this event can cause

kejadian berakibat pada gangguan Operasional Bank dan nasabah. Batas waktu untuk proses secara manual adalah sbb:

- 1-jam untuk transaksi dengan *cut-off time* sebelum pukul 2.30pm
- 2-jam untuk transaksi dengan *cut-off time* setelah pukul 2:30pm

problem in operational system Bank and Customer. Time limit of for manual process are as follows :

- 1-hour for transaction with cut-off time before 2.30pm
- Two-hour for transaction with cut-off time after 2.30pm

E.gTransaksi *Remittance* untuk pengiriman transaksi dalam mata uang *JPY* harus dilakukan manual paling lambat pukul 10:00 am.

Dalam hal kondisi darurat, Kepala Divisi TI akan berkoordinasi dengan Koordinator *Contingency Planning* untuk melakukan tindakan yang dianggap perlu.

E.g Remittance transaction for sending the transaction in JPY currency must be do manual at the latest hour 10:00 am.

In terms of the state of emergency, IT Division Head will coordination with Contingency Planning Coordinator for doing the important action.

4. Kepala Divisi TI akan menginformasikan kepada Departemen/divisi terkait dan jika diperlukan akan mengirimkan informasi permasalahan sistem TI yang terjadi ke nasabah dengan menggunakan aplikasi *Docoblast.*

4. IT division head will inform to the related Department/division and if it is requierd he/she will sending the information about IT system problem occured to customer using Docoblast. Application.

5. Kepala Divisi TI akan mengkoordinasikan kepada Fungsi Operasional dan Dukungan TI, *vendor* dan Departemen/divisi terkait untuk penanganan permasalahan/gangguan yang ada serta pelaksanaan rencana daruratnya.

5. Head Division of IT will coordinating the IT Support & Operational function, vendor and related Department/division for handle the issue/obstacles and then do the emergency plan.

6. Kepala Divisi TI akan memastikan penanganan permasalahan/gangguan sudah berjalan sesuai dengan prosedur dan kebijakan yang berlaku.

6. Head Division of IT will make sure the handling of the issue/problem already running compatible with the procedure and policy which is valid.

7. Dalam hal kondisi darurat sudah dapat diatasi, Kepala Divisi TI akan mengkoordinasikan kepada Fungsi Operasional dan Dukungan TI, *vendor* dan Departemen/Divisi terkait untuk proses melakukan perbaikan/*recovery* sistem yang bermasalah, mengacu pada pedoman *DRP* terkait.

7. In terms of the state of emergency can be handled, Head of IT Division will coordinating IT Support & operational function, vendor and related Department/division for doing the recovery proccess of system which problem with refers to .related DRP guidelines.

IV. PENILAIAN RISIKO

Penilaian risiko diperlukan Bank untuk dapat menilai fungsi yang kritikal sehingga bisnis operasional terus berjalan, mendefinisikan kontrol yang sesuai dan biaya yang dibutuhkan dalam kontrol.

A. Analisis Dampak Gangguan/Bencana terhadap Industri Keuangan

Divisi yang mengelola risiko secara harian harus menganalisa timbulnya risiko akibat bencana sebagai berikut:

IV. RISK ASSESSMENT

Risk assessment is required by Bank to assess critical function to ensure continuity of business operation, define a proper control and cost control.

A. Impact Analysis of Disturbance/ Disaster to Financial Industry

Division that managed daily risk that has to analyze risk caused by disaster are as follow:

Tipe Risiko ***Risk Type***	**Divisi Terkait** ***Related Division***
Risiko Kredit *Credit Risk*	Divisi Credit Portfolio Management (Departemen Credit Portfolio & Analytics Department)
Risiko Likuiditas *Liquidity Risk*	Risk Management Division
Risiko Reputasi *Reputation Risk*	Planning & Finance Division
Risiko Hukum *Legal Risk*	Legal Department
Risiko Operasional Sistem *System Operation Risk*	IT Division

1. Risiko Kredit

Apabila timbulnya bencana mengakibatkan nasabah mengalami kesulitan untuk memenuhi kewajibannya. Tindakan yang harus dilakukan adalah:

a. Mengumpulkan data-data nasabah yang terkena bencana.

b. Meminta informasi mengenai seberapa besar kerusakan yang diakibatkan oleh bencana. Apabila diperlukan melakukan pemeriksaan secara langsung dengan didampingi oleh perusahaan *appraisal*.

c. Melaporkan kepada Direksi mengenai hasil dari penilaian dan pemeriksaan tersebut.

1. Credit Risk

If disaster causing customer having difficulties in fulfill responsibility. Following is action plan:

a. Collect customer data that affected by disaster.

b. Ask information about the damaged that caused by disaster. If necessary conduct assessment accompanied by appraisal company.

c. Report to Board of Directors about result of assessment and inspection.

2. Risiko Likuiditas

Risiko Likuiditas timbul apabila Bank harus mengorbankan likuiditasnya untuk memulihkan lagi aktivitas usahanya. Tindakan yang harus dilakukan adalah:

a. Memonitor secara hati-hati dana yang tersedia di Bank.

b. Mempersiapkan simulasi *Reprising Profile* apabila dibutuhkan sebagai dasar pengambilan keputusan peminjaman dana tambahan.

3. Risiko Reputasi

Risiko reputasi timbul apabila dampak bencana menimbulkan pemberitaan yang negatif mengenai Bank. Tindakan yang harus dilakukan adalah:

a. Memonitor pemberitaan di media massa.

b. Mengingatkan kepada seluruh karyawan mengenai pembatasan informasi keluar, terutama terhadap *pers*.

c. Apabila terdapat pemberitaan yang negatif, segera informasikan kepada Direktur Manajemen Risiko sebelum melakukan tindak lanjut.

4. Risiko Hukum

Risiko hukum timbul apabila timbulnya bencana mengakibatkan adanya tuntutan hukum, ketiadaan peraturan perundang-undangan yang mendukung dalam keadaan darurat, tidak dipenuhinya syarat sahnya kontrak dan pengikatan agunan yang tidak sempurna.

5. Risiko Sistem Operasional

Risiko sistem timbul apabila bencana mengakibatkan terganggunya sistem atau sistem tidak dapat digunakan untuk memproses transaksi dalam periode waktu tertentu.

2. Liquidity Risk

Liquidity Risk if Bank have to give its liquidity to recover business activity. Following is action plan:

a. Monitor carefully fund in Bank

b. Prepare Reprising Profile simulation if required as base for decision making of additional fund.

3. Reputation Risk

Reputation risk occurs if disaster impact is negative news about Bank. Following is action plan:

a. Monitoring news at mass media.

b. Remind to all employee about limiting information especially to pers.

c. If there is negative news, immediately inform to Director in charge of Risk Management before conduct action plan.

4. Legal Risk

Legal risk occurs if disaster causing legal action, no force majeure regulation, no fulfillment of agreement and inadequate collateral agreement.

5. System Operation Risk

System risk occurs if disaster causing system disturbance or system is unavailable to process transaction in certain period.

B. Analisis Berdasarkan Kemungkinan Gangguan/Bencana

B. Analysis based on Disturbance/ Disaster Likelihood

LIKEHOOD	IMPACT				
	Catastrophic (5)	Major (4)	Moderate (3)	Minor (2)	Insignificant (1)
Almost Certain (5)	High	High	Moderate High	Moderate High	Moderate
Likely (4)	High	Moderate High	Moderate High	Moderate	Low Moderate
Moderate (3)	Moderate High	Moderate High	Moderate	Low Moderate	Low Moderate
Unlikely (2)	Moderate High	Moderate	Low Moderate	Low Moderate	Low
Rare (1)	Moderate	Low Moderate	Low Moderate	Low	Low

Penilaian Risiko berdasarkan jenis gangguan dan bencana adalah seperti tabel berikut :

Risk-Assessment according to type of disruption and disaster are as follows :

No	Gangguan/Bencana (Disruption/Disaster)	Lokasi (Location)	Kemungkinan (Likelihood)	Dampak (Severity)	Risiko (Risk)	Dampak / Kerusakan / Kehilangan
1	Kebakaran (Fire)	Data Center	Unlikely	Major	Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan
		Kantor - Pusat	Unlikely	Major	Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor - Cabang dan Cabang Pembantu	Unlikely	Minor	Low	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan
2	Banjir (Flood)	Data Center	Rare	Major	Low Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan
		Kantor - Pusat	Rare	Major	Low Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor - Cabang dan Cabang Pembantu	Rare	Minor	Low	Dokumen, Fixed Asset, Employees
3	Gempa Bumi < 7 SR (Earthquake < 7SR)	Data Center	Moderate	Minor	Low Moderate	Tidak ada kerusakan atau gangguan
		Kantor - Pusat	Moderate	Minor	Low Moderate	Tidak ada kerusakan atau gangguan
		Kantor - Cabang dan Cabang Pembantu	Moderate	Minor	Low Moderate	Tidak ada kerusakan atau gangguan
	Gempa Bumi >= 7 SR (Earthquake >= 7SR)	Data Center	Rare	Major	Low Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan
		Kantor - Pusat	Rare	Major	Low Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor - Cabang dan Cabang Pembantu	Rare	Minor	Low	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan
4	Gangguan Listrik	Kantor - Cabang dan Cabang Pembantu	Unlikely	Minor	Low Moderate	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan
5	Tsunami	Data Center	Rare	Major	Low Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan
		Kantor - Pusat	Rare	Major	Low Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor - Cabang dan Cabang Pembantu	Rare	Minor	Low Moderate	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan
6	Kerusuhan / Huru Hara / Vandalisme	Data Center	Unlikely	Major	Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan
		Kantor - Pusat	Unlikely	Major	Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor - Cabang dan Cabang Pembantu	Unlikely	Minor	Low Moderate	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan

7	Demonstrasi	Data Center	Unlikely	Moderate	Low Moderate	Tidak ada kerusakan atau gangguan; Akses ke Lokasi terganggu
		Kantor - Pusat	Moderate	Moderate	Moderate	Tidak ada kerusakan atau gangguan; Akses ke Lokasi terganggu
8	Pemberontakan	Data Center	Rare	Major	Low Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan.
		Kantor - Pusat	Rare	Major	Low Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor - Cabang dan Cabang Pembantu	Rare	Moderate	Low Moderate	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan
9	Teroris	Data Center	Rare	Major	Low Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan tidak dapat digunakan.
		Kantor - Pusat	Rare	Major	Low Moderate	Aktifitas pada Kantor Pusat tidak dapat dilakukan
		Kantor Cabang dan Cabang Pembantu	Rare	Minor	Low	Aktifitas pada Kantor Cabang dan Cabang Pembantu tidak dapat dilakukan
10	Wabah Penyakit / Disease Outbreak	Data Center	Rare	Minor	Low Moderate	Server, Sistem Aplikasi, Database, Perangkat Jaringan masih dapat digunakan
		Kantor Pusat	Rare	Major	Moderate	Karyawan yang melakukan Aktifitas pada Kantor Pusat menjadi terbatas , dibagi menjadi dua tim (Split Operation) yakni sebagai berikut ; 1. Work From Office (WFO) dan; 2. Work From Home (WFH).
		Kantor Cabang dan Cabang Pembantu	Rare	Major	Moderate	Karyawan yang melakukan Aktifitas pada Kantor Cabang dan Kantor Cabang Pembantu menjadi terbatas. dibagi menjadi dua tim (Split Operation) yakni sebagai berikut : 1. Work From Office (WFO) dan; 2. Work From Home (WFH). Untuk Kantor Cabang Pembantu dilakukan penutupan sebagian.

Skenario penanganan karena adanya gangguan / bencana adalah sebagai berikut:

1. Pemindahan Pusat Data ke lokasi DRC, dalam hal adanya gangguan/bencana yang mengakibatkan kerusakan pada data center sehingga sistem di data center tidak dapat diakses.

2. Mengalihkan layanan dukungan TI kantor pusat/ cabang/cabang pembantu yang terkena dampak gangguan/bencana ke kantor Bank terdekat atau kantor Bank lainnya.

3. Mempersiapkan tim untuk pemulihan pusat data atau kantor Bank yang terdampak gangguan/bencana setelah rencana kontijensi berjalan sesuai

The scenario handling because of a distractions/ disaster is as follows :

1. Relocated Data Center to the DRC Location, in terms of existence a trouble/disaster that can cause a damage in Data Center so that the system in data center cant be access.

2. Diverting IT support services for the head office/branch/sub-branch affected by the disruption/disaster to the nearest Bank office or other Bank offices.

3. Preparing the team for recovery data center or office Bank which affected disorder/disaster after contingency plan runs according

dengan rencana.

plan.

C. Analisis Dampak Gangguan/Bencana

C. Impact Analysis of Disturbance/ Disaster

1. Dampak dari Gangguan/ Kerusakan Server berdasarkan Tingkat Ketersediaan Sistem

1. Impact from Server Disturbance/ Failure based on System Availability Level

Sistem/*System*	Tingkat Ketersediaan Sistem/ *System Availability Level*	Dampak/*Impact*	Transaksional / Non-Transaksional *Transactional / Non-Transactional*
Equation	*Highest*	Operasional Bank terganggu karena tidak dapat memproses semua transaksi nasabah. *Bank operations will be disturbed because could not process all customers transaction*	Transaksional
RTGS/SSSS Gen II/ETP	*Highest*	Bank tidak dapat mengirim/menerima transaksi menggunakan sistem *RTGS* *Bank could not send/receive transaction using RTGS system*	Transaksional
RTGS/SSSS Gen II Interface	*Highest*	Bank tidak dapat mengirim/menerima transaksi menggunakan sistem *RTGS* *Bank could not send/receive transaction using RTGS system*	Transaksional
SKN	*Highest*	Bank tidak dapat mengirim/menerima transaksi menggunakan sistem *SKN* *Bank cannot send/receive transaction using SKN system*	Transaksional
Swift Alliance Entry	*Highest*	Bank tidak dapat melakukan transaksi antar Bank *Bank cannot do interbank transaction*	Transaksional
FBTI	*Highest*	*User* (*Remittance*, *Import*, *Export*, Kantor Cabang) tidak dapat melakukan transaksi *trade finance* *User (Remittance, Import, Export, Branch Office) cannot process trade finance transaction*	Transaksional
Internet Banking PrimeCash	*Highest*	Nasabah tidak dapat melakukan transaksi menggunakan *Internet Banking*, sehingga nasabah harus melakukan transaksi secara manual atau melalui *Fax*. *Customer cannot do transaction using Internet Banking, so customer has to do manual transaction or by fax facility*	Transaksional
ISE	*Highest*	Nasabah tidak dapat terotentikasi untuk dapat terkoneksi ke aplikasi *Internet Banking* *Customer is unable to authenticated to connect to Internet Banking application*	Transaksional
FBMM	*Highest*	Aplikasi *Internet Banking* tidak dapat terhubung ke sistem *Core Bank*, sehingga transaksi nasabah yang melalui *Internet Banking* tidak dapat diproses secara otomatis	Transaksional

		Internet Banking application cannot connect to core banking system, so customer transaction thru Internet Banking cannot be processed automatically	
Velis	*Highest*	Nasabah tidak dapat *release* transaksi *Internet Banking* karena sistem *token* terganggu. *Customer cannot release Internet Banking transaction because token system is disturbed*	Transaksional
MPN Gen 3	*Highest*	Pembayaran *billing* pajak tidak dapat diproses *Tax billing payment cannot be processed*	Transaksional
Domain	*Highest*	Semua *user* tidak dapat *login* ke jaringan Bank *All user cannot login to Bank network*	Non-Transaksional
PSAK 71	*Highest*	*User* (Divisi Credit Exam, Divisi Kredit, Departemen Akunting, Kantor Cabang) tidak dapat mengeluarkan data untuk pelaporan *User (Credit Exam Division, Credit Division, Accounting, Branch Office) cannot generate data for reporting*	Non-Transaksional
BI Reporting - LBUT *BI Reporting - LLD* *BI Reporting - SLIK* *BI Reporting - Antasena* *Fusion Risk*	*High*	Tidak dapat mengirimkan laporan ke BI, OJK *Could not send report to BI, OJK*	Non-Transaksional
VPN	*High*	User WFH tidak dapat terkoneksi jaringan kantor *WFH users cannot connect to the office network*	Non-Transaksional
E-statement	*Middle*	Proses pengiriman *e-statement* terganggu *E-statement process delivery is disturbed*	Non-Transaksional
Web Teller	*Middle*	Proses di *front office* terganggu *Front office process is disturbed*	Transaksional
APU-PPT	*Middle*	*User* (APU-PPT, Cabang) tidak dapat mengirimkan laporan untuk *PPATK* *User (APU-PPT, Branch) cannot send report to PPATK*	Non-Transaksional
Sipendar	*Middle*	*User* APU-PPT tidak dapat mengakses aplikasi *website* Pertukaran Informasi Pendanaan *Terorisme* *APU-PPT users cannot access the Terrorism Financing Information Exchange website application*	Non-Transaksional
Bloomberg	*Middle*	*User* (*Treasury)* tidak dapat melakukan transaksi valuta asing *User (Treasury) cannot conduct foreign exchange transaction*	Transaksional
CRS	*Middle*	*User* tidak dapat mengelola risiko kredit *User cannot manage credit risk*	Non-Transaksional
DHIB	*Middle*	Bank tidak dapat mengakses *DHIB* *Bank cannot access to DHIB*	Non-Transaksional
Email	*Middle*	*User* tidak dapat mengirim/menerima *email* *User cannot send/receive email*	Non-Transaksional
File Server	*Middle*	*User* tidak dapat mengakses *file* yang digunakan dalam aktivitas sehari-hari *User cannot access file that is used for daily*	Non-Transaksional

		activity	
GO AML	*Middle*	*User* tidak dapat mengirimkan laporan ke PPATK *User cannot send report to PPATK*	Non-Transaksional
Market Risk	*Middle*	*User* tidak dapat mengelola risiko pasar *User cannot manage market risk*	Non-Transaksional
PABX	*Middle*	Sistem telepon terganggu *Telephone system is disturbed*	Non-Transaksional
QMS	*Middle*	Antrian di *front office* tidak dapat dilakukan menggunakan sistem *Queuing at front office cannot be done by system*	Non-Transaksional
RBC	*Middle*	*Rating* nasabah tidak dapat diakses *Customer rating cannot be accessed*	Non-Transaksional
CIS	*Middle*	Memo kredit dan fasilitas kredit tidak dapat diproses *Memo credit and credit facility cannot be processed*	Non-Transaksional
SMART-SVS	*Middle*	*User* tidak dapat melakukan verifikasi tandatangan nasabah *User cannot verify customer signature*	Non-Transaksional
Symantec Backup Exec	*Middle*	Tidak dapat melakukan *backup* harian *Cannot conduct daily backup*	Non-Transaksional
Symantec End Point	*Middle*	*Update* antivirus tidak dapat dilakukan *Update antivirus cannot be done*	Non-Transaksional
VoIP	*Middle*	Tidak dapat menggunakan telepon IP ke Cabang *Cannot use IP phone to Branch*	Non-Transaksional
Kaspersky	*Middle*	Update antivirus tidak dapat dilakukan *Update antivirus cannot be done*	Non-Transaksional
Groupware (Intramart)	*Middle*	*User* tidak dapat mengakses *workflow* dan dokumen internal *User cannot access workflow and internal document*	Non-Transaksional
Bsafe	*Unclassified*	*Monitoring log Equation* tidak dapat dilakukan *Cannot monitoring Equation log*	Non-Transaksional
CCTV	*Unclassified*	Tidak ada rekaman keamanan *There is no security footage*	Non-Transaksional
Elearning	*Unclassified*	*User* tidak dapat menggunakan *e-learning* *User cannot use e-learning*	Non-Transaksional
HRIS	*Unclassified*	Data karyawan tidak dapat diakses *Employee data could not be access*	Non-Transaksional
JP1	*Unclassified*	Tidak dapat melakukan inventaris secara otomatis *Could not do automatic inventory*	Non-Transaksional
PACOM Access Control	*Unclassified*	Tidak dapat mengakses ruangan/area *Could not access room/area*	Non-Transaksional
NRX Voice Recording	*Unclassified*	Tidak dapat merekam telepon masuk/keluar *Could not record incoming/outgoing phone*	Non-Transaksional
Operational Risk	*Unclassified*	*User* tidak dapat mengelola risiko operasional *User could not manage operational risk*	Non-Transaksional
Smart2K	*Unclassified*	*User* tidak dapat melakukan absen sidik jari *User cannot use finger print attendance*	Non-Transaksional

OCR	*Unclassified*	*User* tidak dapat melakukan *scan* dokumen rahasia nasabah (seperti jaminan, akta, dan lainnya) *User cannot scan customer confidential document (such as collateral, certificate and others)*	Non-Transaksional
Whatsup Gold	*Unclassified*	Divisi TI tidak dapat melakukan *monitoring* jaringan menggunakan sistem *IT Division cannot monitor network by system*	Non-Transaksional
DocoBlast	*Unclassified*	*User* tidak dapat mengirimkan *email broadcast* ke nasabah *User cannot send broadcast email to customer*	Non-Transaksional
Fastrack	*Unclassified*	*User* tidak dapat mengakses daftar *fixed asset* *User cannot access fixed asset list*	Non-Transaksional
CaseWare IDEA	*Unclassified*	*User* tidak dapat menggunakan sistem sebagai alat tambahan untuk analisis audit *User cannot use system as additional tools for audit analysis*	Non-Transaksional

- ***Highest*****:** Sistem yang harus dipastikan ketersediannya, sistem terkait penyelesaian transaksi nasabah, jaringan atau sistem pemrosesan data internal.
- ***High*****:** Sistem yang memiliki prioritas utama dalam menunjang operasional Bank.
- ***Middle:*** Sistem yang memiliki prioritas rendah dalam operasional Bank dan keberlangsungan pekerjaan digantikan oleh manual proses atau penggunaan sistem lainnya.
- ***Unclassified*****:** Sistem selain klasifikasi di atas.

- **Highest**: System that need ensure its availability, system related to customer transaction settlement, network or internal data processing system.
- **High**: System that has advance priority in operational Bank.
- **Middle**: System that has low priority in operational Bank and continuation work based on manual process or the use of other system.
- **Unclassified**: System others than above classification.

2. Dampak dari Gangguan/ Kerusakan Jaringan Komunikasi Data

2. Impact from Data Network Communication Disturbance/ Failure

Jaringan / Network	Analisa Dampak / Impact Analysis
WAN (FO Channel/LAN)	• Kantor Pusat Menara Mulia, Kantor Cabang dan Cabang Pembantu tidak dapat terhubung ke *Data Center* *Head Office Menara Mulia, Branch Office and Sub Branch Office cannot connect to Data Center* • *Client* (*Workstation*), PC/Laptop tidak dapat terhubung melalui jaringan FO ke *Data Center* *Client (workstation), PC/Laptop cannot connect thru FO network to Data Center* • Tidak dapat mengakses *server* *Cannot access server*
MPLS (IP VPN)	• Cabang/Capem tidak dapat terhubung ke *Data Center* *Branch/Sub Branch cannot connect to Data Center* • VoIP tidak dapat digunakan *VoIP is cannot be used* • Harus menggunakan *backup line* *Have to use backup line*

Meskipun gangguan/kerusakan jaringan tidak mempunyai dampak langsung pada *hardware* atau sistem, gangguan/kerusakan dapat mengakibatkan keterlambatan proses operasional dan mengganggu aktivitas bisnis perusahaan. Jaringan komunikasi harus diuji minimal setahun sekali terutama yang berhubungan dengan aplikasi *Core Banking*.

Even though network disturbance/failure has no direct impact to hardware or system, disturbance/damage could cause delay in operational process and disturb business activity. Network communication should be tested once a year, especially network related to Core Banking application.

3. Analisa Dampak Gangguan/Bencana terhadap Nasabah dan Bank

Gangguan/bencana memiliki dampak terhadap nasabah dan juga Bank, sebagai berikut:

a. Pengaduan nasabah yang dapat mengakibatkan risiko reputasi.

b. Mengurangi tingkat kepercayaan nasabah.

c. Nasabah menarik dananya dari Bank dan memindahkannya ke Bank lain.

d. Kemungkinan penarikan besar-besaran (*rush*)

e. Likuiditas Bank terganggu karena dana pihak ketiga berkurang.

f. Nasabah menuntut Bank dan akan berakibat risiko hukum.

g. Transaksi Nasabah terganggu/*delay*.

3. Impact Analysis of Disturbance/ Disaster to Customer and Bank

Disturbance/disaster impact to customer and Bank as follow:

a. Customer complains that can cause reputation risk.

b. Decrease customer trust.

c. Customers withdraw the fund and transfer to another Bank.

d. Potential rush.

e. Bank liquidity is disturb because of third party fund is decrease.

f. Customer sues Bank and will cause legal risk.

g. Customer transaction is delay/disturb.

V. PENYUSUNAN BCP

A. Prosedur BCP

Tindakan yang dilakukan ketika terjadi gangguan/bencana mengacu pada

1. Pedoman *Disaster Recovery Plan* Aplikasi RTGS G2
2. Pedoman *Disaster Recovery Plan* Aplikasi SKNBI Gen-2
3. Pedoman *Disaster Recovery Plan (DRP)* MPN G2
4. Pedoman *Disasater Recovery Plan* Internet Banking.
5. Pedoman *Business Continuity Plan* Sistem *Core Banking*
6. Pedoman *Disaster Recovery Plan* Aplikasi Smart SVS
7. Pedoman *Disaster Recovery Plan* CIS

B. Alur Komunikasi

Daftar telepon yang digunakan untuk alur komunikasi pada suatu Divisi merupakan tanggung jawab dari masing-masing Kepala Divisi untuk melakukan pengkinian daftar nomor telepon, sedangkan untuk Kantor Cabang tanggung jawab untuk melakukan pengkinian berada pada Kepala Kantor Cabang terkait.

C. Komponen BCP

1. Personil

   Kepala Departemen/Divisi/Cabang menentukan personil yang bertanggung jawab dalam proses BCP termasuk menetapkan alur komunikasi dalam keadaan gangguan/darurat.

2. Teknologi

   Peralatan dan *hardware* mempunyai perjanjian pemeliharaan dengan Vendor yang beragam. Oleh karena itu diperlukan suatu SLA (*Service Level Agreement*) yang mencakup

V. CREATING BCP

A. BCP Procedure

Action taken during disturbance/disaster refer to

1. A Guidance Disaster Recovery Plan of RTGS G2 Application
2. DRP Guidance of SKNBI-Gen2 Application
3. Disaster Recovery Plan of MPN G2 Guideline
4. Internet Banking Disaster Recovery Plan Guideline
5. Business Continuity Plan of Core Banking System Guidelines
6. Disaster Recovery Plan Smart SVS Aplication Guideline
7. Disaster Recovery Plan CIS Application Guideline

B. Communication Tree

List of phone numbers that use for Communication Tree in a Division is the responsibility of each Head of Division, while for the responsibility of Branch Office to updating is at the Head of Branch Office.

C. BCP Component

1. Personnel

   Head of Department/Division/Branch assign personnel that responsible in BCP process includes determine communication tree in emergency.

2. Technology

   Tools and hardware have a different maintenance agreement. Therefore it is require SLA (Service Level Agreement) that cover scope of work, maintenance service, response time,

lingkup perkerjaan, layanan pemeliharaan, waktu tanggap, tingkat kinerja, dan lainnya. Semua *software* dan *hardware* yang kritikal harus dievaluasi minimal setahun sekali.

performance level and others. All critical software and hardware are evaluated at least once a year.

3. *Disaster Recovery Center*

   Bank memiliki *Disaster Recovery Center* yang dapat digunakan dalam keadaan gangguan/darurat dan memiliki prosedur pemulihan sistem operasional di lokasi *Disaster Recovery Center.*

   Disaster Recovery Center dapat dikelola sendiri ataupun oleh pihak penyedia jasa. Dalam pemilihan *DRC* Bank mempertimbangkan hal sebagai berikut

   a. Letak geografis *DRC*

   b. Analisa risiko terkait dengan lokasi *DRC*

   c. Ketersediaan jaringan komunikasi dan listrik yang dapat menjamin operasional *DRC*

   d. Kesesuaian sistem di *Data Center* dengan *DRC*

   e. Prosedur pengamanan di *DRC*

   f. Analisa lokasi *DRC* terkait proses *recovery*

3. Disaster Recovery Center

   Bank has Disaster Recovery Center that is use in emergency and has recovery procedure for operational system at Disaster Recovery Center

   Disaster Recovery Center is self-maintain or by provider. In selecting DRC, Bank consider the following:

   a. Geographic DRC

   b. Risk analysis of DRC location

   c. Availability of network communication and electricity to support DRC operation

   d. System compatibility at Data Center and DRC.

   e. Security procedure at DRC

   f. DRC location analysis related to recovery process

4. *Backup*

   a. *Backup* data harian dilakukan oleh Fungsi Operasional & dukungan TI. *Backup* data dilakukan ketika EOD (*end of day*) diluar *backup* insidentil. Untuk *backup* data mingguan atau bulanan telah dicantumkan pada *checklist*.

   b. Proses *backup* dibagi menjadi proses *backup* sebagian atau *backup* keseluruhan. *Backup* sebagian memerlukan waktu yang lebih sebentar dibandingkan *backup* keseluruhan.

4. Backup

   a. Daily backup data is done by IT Support & Operational Function. Backup data is done during EOD (end of day) outside incidental backup. For weekly or monthly backup is in checklist.

   b. Backup process is divided into temporary or permanent backup. Temporary backup require shorter time than permanent backup.

c. Personil Fungsi Operasional & Dukungan TI yang melakukan proses *backup* data bertanggung jawab untuk mengikuti prosedur *backup* termasuk penggunaan media penyimpanan (CD, Disket, ZIP, *Flash Disk*, LTO), *register* media dan metode *transfer* data media untuk *offsite*.

c. IT Support & Operational function personnel that processing backup data is responsible to follow backup procedure includes in the use of storage media (CD, Diskette, ZIP, Flash Disk, LTO), register media and transfer media data method for offsite backup.

d. Proses *backup* mengacu ke *SOP IT Daily Operation*.

d. Backup process refers to SOP IT Daily Operation.

e. Divisi Teknologi Informasi memastikan bahwa data yang di*backup* dapat di-*restore* ketika diperlukan dengan melakukan *test restore* secara berkala, dan *update software* atau sistem dilakukan jika ada perubahan pada mesin produksi.

e. Information Technology Division ensure that backup data can be restore at any time by doing periodic restore test and update software or system is done if there is changes at production machine.

5. *Business Recovery Center (BRC)*/*Crisis Center*/*Business Resumption Center*

BCP harus memiliki skenario mengenai lokasi kegiatan dari masing-masing fungsi bisnis untuk berbagai tingkat *disaster*. Untuk tingkat bencana *total disaster* atau *catasthropic*, Bank sebaiknya menyiapkan lokasi alternatif agar tetap dapat menjalankan kegiatan fungsi bisnis.

Untuk memastikan keberlangsungan kondisi BRC yang memadai dan dapat beroperasional sewaktu-waktu dibutuhkan, perlu dilakukan pengecekan pada area BRC minimal 6 bulan sekali.

5. Business Recovery Center (BRC)/Crisis Center/Business Resumption Center

BCP must have scenario about each location activity for each business function for any level of disaster. For total disaster or catastrophic, Bank should prepare alternative location to continue business process.

To ensure the continuity of adequate and operational BRC conditions whenever needed, it is necessary to check the BRC area at least once every 6 months.

6. Jaringan Komunikasi Alternatif

Bank harus memastikan bahwa alternatif jalur komunikasi yang terdapat di wilayah operasional Bank dapat digunakan pada saat gangguan/bencana, baik di lingkungan *intern* maupun dengan pihak *ekstern*.

6. Alternative Communication Network

Bank should ensure that alternative communication network at alternative location can be used during disturbance/disaster, both internal and external network.

VI. PENGUJIAN BCP

A. Ruang Lingkup

1. Pengujian evakuasi dan alur komunikasi.
2. Penentuan kondisi bencana dilakukan oleh *Direktur in Charge*.
3. Pengujian disesuaikan dengan fasilitas yang ada pada *Data Center* dan *DRC*.
4. Pengujian pemulihan data penting.
5. Pengembalian kegiatan operasional Bank dan *Data Center* ke lokasi unit bisnis dan pusat data semula.
6. Uji coba dilakukan minimal setahun sekali, diinisiasi oleh Tim BCM dengan melibatkan Divisi Teknologi Informasi dan *end user*.

B. Skenario Pengujian

1. Metode

Berikut adalah contoh metode yang dapat digunakan dalam pengujian BCP. Skenario hendaknya di-*update* seiring dengan perkembangan bisnis dan dilakukan minimal satu kali dalam setahun.

a. Pengujian *BCP* secara mendadak menggunakan alur komunikasi di setiap Departemen/Divisi/Cabang.

b. Melakukan simulasi keadaan gangguan/bencana.

c. Pengujian *BCP* untuk unit bisnis tertentu.

d. Pengujian *BCP* dari sisi teknikal sistem dan proses informasi.

e. Pengujian *BCP* untuk seluruh unit bisnis dan Divisi TI.

VI. BCP TESTING

A. Scope

1. Evacuation drill and communication tree
2. Director in Charge is responsible to determine disaster condition.
3. Testing adjust with facility at Data Center and DRC.
4. Restore critical data
5. Recover Bank operational activity and Data Center to business unit location and data center.
6. Test is conduct at least once a year, initiate by Business Continuity Management Division by involving Information Technology Division and end user.

B. Testing Scenario

1. Method

Following is example of method for testing BCP. Scenario should be updated base on the development of business and conduct at least once a year.

a. BCP testing using emergency communication tree at each Department/Division/Branch.

b. Evacuation drill.

c. BCP testing for certain business unit.

d. BCP testing from technical and information process point of view.

e. BCP testing for all business unit and IT Division.

2. Tujuan

Skenario pengujian *BCP* dibuat dengan tujuan sebagai berikut:

a. Untuk menentukan waktu yang digunakan dalam penyampaian berita keadaan gangguan/darurat.

b. Untuk memastikan kesiapan prosedur *BCP* dan komponen *BCP*.

c. Untuk melakukan verifikasi *BCP* berdasarkan kebutuhan bisnis.

d. Untuk menetapkan dan mendokumentasikan masalah yang terjadi dalam proses pengujian *BCP* (personil, teknologi, *DRC*, *restore* proses dan *backup* proses).

C. Analisa dan Hasil Pengujian BCP

Divisi Teknologi Informasi membuat laporan hasil pengujian *BCP* sebagai berikut:

1. Tujuan dan skenario pengujian.
2. Tanggal pelaksanaan.
3. *Person in Charge.*
4. Deskripsi mengenai kesenjangan antara Rencana Pemulihan Bencana dan hasil pengujian serta usulan perubahannya.
5. Hasil pengujian (gagal/berhasil).
6. Tindakan perbaikan untuk mengatasi permasalahan yang terjadi.
7. Kesimpulan.
8. Rekomendasi untuk pengujian selanjutnya .

2. Purpose

The purpose of creating BCP testing scenario

a. To determine required time for communication tree process.

b. To ensure readiness of BCP procedure and BCP component.

c. To conduct BCP verification base on business requirement.

d. To determine and documented problem during BCP testing process (personnel, technology, DRC, restore process and backup process).

C. Analysis and Result of BCP Testing

Information Technology Division create report of BCP result as follow:

1. Testing purpose and scenario.
2. Implementation date.
3. Person in charge.
4. Description about gap between Disaster Recovery Plan and testing result include suggestion for revision.
5. Testing result (fail/success).
6. Corrective action to solve problem occurred during testing.
7. Conclusion.
8. Recommendation for next testing.

VII. PEMELIHARAAN BCP

Divisi Manajemen Risiko bekerja sama dengan Divisi Teknologi Informasi dan Departemen Pengawas Keamanan Informasi dan Risiko Sistem untuk pengkinian dokumen untuk kemudian diketahui oleh Divisi Manajemen Risiko sebagai berikut:

1. Latihan dalam keadaan darurat
2. Alur komunikasi
3. *Self assessment* antara *BIA* dan kondisi saat ini
4. Analisa dari proses bisnis kritikal, struktur organisasi, sistem, *software*, OS, *hardware*, *personil*, *vendor.*
5. Melakukan pelatihan kepada *personil* BRP.

VII. BCP MAINTENANCE

Risk Management Division cooperate with Information Technology Division and Information Security and System Risk Controller Department to update document as follow:

1. Evacuation drill
2. Communication tree
3. Self-assessment between BIA and current condition
4. Analysis of critical business process, organization structure, software, OS, hardware, personnel, vendor
5. Conduct training to BRP personnel.

VIII. INTERNAL AUDIT

Pemeriksaan kesesuaian *BCP*, kecukupan *BCP* dan/atau efektifitas pengujian *BCP* dilakukan oleh Internal Audit. Untuk prosedur pemeriksaan mengacu ke Kebijakan Audit *Intern* Teknologi Informasi.

VIII. AUDIT INTERN

Assess BCP adequacy, suitability and/or effectiveness of BCP testing is done by Internal Audit. For assessment procedure refers to Information Technology Internal Audit Policy.

IX. PENUTUP

Kebijakan *Business Continuity Plan* Operasional Sistem 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.

Kebijakan Business Continuity Plan Operasional Sistem ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur pada tanggal 6 Juli 2023 dan Dewan Komisaris pada tanggal 2 Agustus 2023 serta mencabut Kebijakan *Business Continuity Plan* Operasional Sistem Edisi 9, Mei 2022

Kebijakan ini akan dikaji ulang secara berkala paling lambat setiap 2 (dua) tahun sekali atau jika diperlukan sebagai upaya penyempurnaan sesuai dengan perkembangan usaha dan kebutuhan Bank atau perubahan peraturan yang mendasarinya.

IX. CLOSING

Business Continuity Plan Policy of Operational System are issued in 2 (two) languages, Indonesia Languages and English Languages, and if there is a different in interpretation between the two, the refferences is indonesia languages.

This System Operational Business Continuity Plan Policy comes into effect after obtaining the approval of the President Director on Date July 6th, 2023 and the Board of Commissioners on Date August 2nd, 2023 and revoking the System Operational Business Continuity Plan Policy Edition 9th , May 2023

This policy will be reviewed at latest every 2 (two) years or if needed as an improvement effort following the business development and the need of Bank or following the changes of base regulation.