SALINAN
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DENGAN RAHMAT TUHAN YANG MAHA ESA

ANGGOTA DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 10, Pasal 11, Pasal 12, Pasal 15, Pasal 16, Pasal 17, Pasal 18, Pasal 34, Pasal 38, Pasal 39, Pasal 43, Pasal 47, Pasal 52, Pasal 57, dan Pasal 65 Peraturan Otoritas Jasa Keuangan Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, serta untuk mendukung kelangsungan operasional dan pelayanan bank dalam pemanfaatan teknologi informasi, perlu menetapkan Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum;

Mengingat : 1. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6845);
2. Peraturan Otoritas Jasa Keuangan Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 5/OJK, Tambahan Lembaran Negara Republik Indonesia Tahun 2022 Nomor 5/OJK);

MEMUTUSKAN:

Menetapkan : PERATURAN ANGGOTA DEWAN KOMISIONER OTORITAS JASA KEUANGAN TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM.

Pasal 1

Ketentuan mengenai penyelenggaraan TI oleh Bank sebagaimana tercantum dalam:

a. Lampiran I yang memuat mengenai pedoman penyelenggaraan teknologi informasi oleh bank umum;
b. Lampiran II yang memuat mengenai tata cara penyampaian laporan dan permohonan izin;
c. Lampiran III yang memuat mengenai format laporan dan notifikasi; dan
d. Lampiran IV yang memuat mengenai format permohonan izin dan laporan realisasi,

yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

Pasal 2

Bank yang telah menggunakan pihak penyedia jasa TI sebelum berlakunya Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini, harus menyesuaikan perjanjian yang telah dibuat sesuai dengan ketentuan dalam Peraturan Anggota Dewan Komisioner ini.

Pasal 3

Penyampaian laporan kondisi terkini penyelenggaraan TI dengan menggunakan format sebagaimana tercantum dalam Lampiran III Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini dilakukan sesuai dengan:

a. ketentuan Otoritas Jasa Keuangan mengenai pelaporan bank umum konvensional melalui sistem pelaporan otoritas jasa keuangan; dan
b. ketentuan Otoritas Jasa Keuangan mengenai pelaporan bank umum syariah dan unit usaha syariah melalui sistem pelaporan otoritas jasa keuangan.

Pasal 4

Pada saat Peraturan Anggota Dewan Komisioner ini mulai berlaku, ketentuan sebagaimana dimaksud dalam Surat Edaran Otoritas Jasa Keuangan Nomor 21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, dicabut dan dinyatakan tidak berlaku.

Pasal 5

Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini mulai berlaku pada tanggal 1 Maret 2026.

Ditetapkan di Jakarta
pada tanggal 23 Januari 2026

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN I
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

PEDOMAN
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DAFTAR ISI
PEDOMAN PENYELENGGARAAN TI OLEH BANK UMUM

BAB I
PENDAHULUAN

Teknologi Informasi (TI) memiliki peranan penting dalam mendukung operasional dan bisnis industri perbankan. Perkembangan TI yang sangat cepat menawarkan beragam alternatif solusi dan kemudahan bagi industri perbankan. Di sisi lain, peningkatan pemanfaatan TI juga dapat memunculkan risiko yang perlu diidentifikasi, dimitigasi, bahkan dikendalikan, sehingga tidak mengganggu bisnis perbankan. Oleh karena itu, Bank perlu memperkuat tata kelola dalam penyelenggaraan TI sehingga pemanfaatan TI dapat memberikan nilai tambah bagi Bank melalui optimalisasi sumber daya untuk memitigasi risiko yang dihadapi oleh Bank. Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (POJK PTI), diperlukan pedoman mengenai penyelenggaraan TI oleh Bank.

Pedoman penyelenggaraan TI berisi penjabaran lebih lanjut dari ketentuan dalam POJK PTI yang dapat menjadi acuan bagi Bank dalam menyelenggarakan TI sesuai dengan POJK PTI. Ruang lingkup dari pedoman penyelenggaraan TI, meliputi:

1. penerapan tata kelola TI;
2. penyusunan arsitektur TI, termasuk rencana strategis TI;
3. penerapan manajemen risiko TI;
4. keamanan dan ketahanan siber;
5. penggunaan pihak penyedia jasa TI;
6. penempatan Sistem Elektronik dan pemrosesan transaksi berbasis TI;
7. pengelolaan data dan pelindungan data pribadi;
8. penyediaan jasa TI oleh Bank;
9. pengendalian dan audit intern TI; dan
10. penilaian tingkat maturitas digital Bank.

Pedoman penyelenggaraan ketahanan dan keamanan siber sebagaimana dimaksud pada angka 4 mengacu pada Surat Edaran Otoritas Jasa Keuangan mengenai Ketahanan dan Keamanan Siber bagi Bank Umum (SEOJK Siber), dan pedoman penilaian maturitas digital bank sebagaimana dimaksud pada angka 10 mengacu pada Surat Edaran Otoritas Jasa Keuangan mengenai Penilaian Tingkat Maturitas Digital Bank Umum (SEOJK DMAB).

BAB II
TATA KELOLA TI BANK

A. Pendahuluan

Pemanfaatan TI oleh Bank bertujuan agar TI dapat memberikan nilai tambah dan selaras dengan strategi bisnis Bank. Tata kelola TI memberikan panduan kerangka kerja dan struktur, yang menghubungkan sumber daya dan informasi TI dengan tujuan dan strategi bisnis. Tata kelola TI bertujuan untuk memastikan bahwa aset TI mendukung tujuan bisnis Bank, melalui perencanaan, pengembangan, penerapan, dan pemantauan kinerja TI yang sesuai dengan *best practices*. Dalam penyelenggaraan TI, Bank wajib menerapkan tata kelola TI yang baik sebagaimana telah diatur dalam Pasal 2 ayat (1) POJK PTI.

Penerapan tata kelola TI merupakan bagian integral dari penerapan tata kelola Bank secara umum. Tata kelola TI diterapkan pada seluruh kegiatan yang berkaitan dengan penyelenggaraan TI antara lain manajemen risiko, ketahanan dan keamanan TI termasuk siber, pengelolaan data, penggunaan Pihak Penyedia Jasa TI (PPJTI), penyediaan jasa TI oleh Bank, pengendalian intern, serta pengembangan dan perubahan pada TI. Penerapan tata kelola TI berlaku bagi seluruh unit dan/atau fungsi pada Bank, baik sebagai pengelola TI maupun pengguna TI.

1. Faktor Penerapan Tata Kelola TI

Dalam menerapkan tata kelola TI yang baik, Bank mempertimbangkan paling sedikit 7 (tujuh) faktor sebagaimana dimaksud dalam Pasal 2 ayat (2) POJK PTI, yaitu:

a. Strategi dan Tujuan Bisnis Bank

Tata kelola TI disesuaikan dengan strategi dan tujuan bisnis dari Bank. Strategi dan tujuan bisnis Bank mencerminkan arah bisnis dan kebutuhan dari pemangku kepentingan (*stakeholders*). Dalam penentuan strategi dan tujuan bisnis, Bank dapat mempertimbangkan antara lain:

1) pertumbuhan bisnis;
2) jenis produk dan/atau layanan yang diberikan, termasuk inovasi bisnis; dan
3) strategi efisiensi biaya.

b. Ukuran dan Kompleksitas Bisnis Bank

Ukuran dan kompleksitas bisnis Bank dapat ditentukan berdasarkan antara lain struktur organisasi, total jumlah pegawai, total jumlah jaringan kantor, serta kompleksitas produk dan layanan yang diberikan.

c. Peran TI bagi Bank

Peran TI bagi Bank mencerminkan seberapa penting TI dalam mendukung bisnis Bank. Beberapa model bisnis yang menunjukkan peran TI bagi Bank antara lain:

1) TI memiliki dampak langsung pada keberlangsungan proses bisnis dan layanan, namun TI belum dianggap sebagai penggerak inovasi proses bisnis dan layanan;
2) TI dianggap sebagai penggerak inovasi proses bisnis dan layanan, namun belum ada ketergantungan kritis pada TI untuk keberlangsungan proses bisnis dan layanan; dan
3) TI memiliki peranan yang sangat penting atau kritikal dalam menjalankan proses bisnis dan layanan.

d. Metode Pengadaan Sumber Daya TI
Metode pengadaan sumber daya TI disesuaikan dengan kebutuhan dan kemampuan Bank, antara lain pengadaan secara mandiri, pengadaan dengan menggunakan PPJTI, dan kombinasi antara keduanya.

e. Risiko dan Permasalahan terkait TI
Penerapan tata kelola TI perlu disesuaikan dengan profil risiko dan permasalahan terkait TI yang dihadapi oleh Bank.

f. Praktik atau Standar yang Berlaku Secara Nasional maupun Internasional
Penentuan praktik atau standar yang berlaku secara nasional maupun internasional yang akan digunakan sebagai dasar penerapan tata kelola TI sesuai dengan kebutuhan dan kemampuan Bank.

g. Ketentuan Peraturan Perundang-Undangan
Penerapan tata kelola TI dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

2. Aspek Tata Kelola TI

Sesuai Pasal 3 Ayat (1) POJK PTI, Bank wajib melakukan pemetaan, perencanaan, dan/atau penetapan atas aspek tata kelola TI. Bank juga memastikan terciptanya sinergi pada seluruh aspek tata kelola TI tersebut. Aspek tata kelola TI, terdiri atas paling sedikit:

a. Proses Bisnis
Proses Bisnis merupakan sekumpulan aktivitas terstruktur yang disusun untuk mencapai tujuan bisnis, serta menghasilkan *output* yang mendukung pencapaian tujuan terkait TI secara keseluruhan. Pada *level governance* (tata kelola) proses bisnis tercermin melalui aktivitas evaluasi atas pilihan strategi, pengarahan atas strategi penyelenggaraan TI, dan pemantauan pencapaian strategi. Sedangkan pada *level management* (manajemen) proses bisnis tercermin melalui aktivitas:
1) penyelarasan, perencanaan, dan pengorganisasian seluruh unit, strategi, dan kegiatan yang mendukung penyelenggaraan TI;
2) pendefinisian, akuisisi, dan implementasi atas solusi TI serta integrasinya dalam proses bisnis Bank;
3) penyediaan dukungan operasional layanan TI kepada pemangku kepentingan; dan
4) pemantauan kinerja dan kesesuaian penyelenggaraan TI dengan target kinerja intern, pengendalian intern, dan ketentuan peraturan perundang-undangan.

b. Struktur Organisasi
Bank harus menetapkan tugas dan tanggung jawab dari setiap jabatan yang terkait pada setiap proses bisnis yang dimiliki Bank dalam penyelenggaraan TI. Dalam menentukan struktur organisasi, Bank perlu menyesuaikan dengan kebutuhan penyelenggaraan dan penggunaan TI, dengan memperhatikan paling sedikit:
1) struktur organisasi secara spesifik menggambarkan garis kewenangan, pelaporan, dan tanggung jawab untuk setiap fungsi TI yang dimiliki, termasuk pihak yang ditunjuk sebagai orang pengganti dalam hal terjadi kekosongan dalam struktur organisasi;
2) struktur organisasi yang tidak membuka peluang bagi siapa pun secara independen untuk melakukan dan/atau

menyembunyikan kesalahan atau penyimpangan dalam pelaksanaan tugas serta dapat menonaktifkan fasilitas sistem keamanan;

3) terdapat prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*) untuk mencegah seseorang mendapat tanggung jawab atas fungsi yang berbeda dan kritikal, sedemikian rupa yang dapat menyebabkan kesalahan tidak mudah dideteksi, misalnya penetapan pegawai yang berbeda sebagai penanggung jawab administrasi pengamanan informasi (*security administrator*) dan penanggung jawab pengembangan TI dengan pegawai yang melakukan kegiatan operasional TI;

4) bentuk pengawasan lain (*compensating controls*) untuk mencegah timbulnya kesalahan terkait penyelenggaraan TI, untuk Bank berskala usaha yang relatif kecil atau kantor cabang di daerah terpencil yang tidak dapat menerapkan prinsip pemisahan tugas dan tanggung jawab yang memadai baik secara keseluruhan maupun sebagian.

   Dalam menentukan bentuk *compensating controls* yang akan diterapkan, Bank perlu memperhatikan kepemilikan data, tanggung jawab otorisasi transaksi, dan hak akses data, contoh *compensating controls* yaitu *audit trail*, rekonsiliasi, *exception reporting*, *transaction log*, *supervisory review*, dan *independent review*. Sekalipun *compensating controls* diterapkan, penyelenggaraan TI tetap harus berdasarkan prinsip kehati-hatian;

5) penempatan personel mempertimbangkan kompetensi Sumber Daya Manusia (SDM), antara lain pengetahuan dan keahlian, yang sesuai dengan posisi jabatan atau tugasnya; dan

6) pembagian tanggung jawab dan penetapan target dirumuskan dengan baik di antara fungsi penerapan manajemen risiko TI dan bidang-bidang fungsional penyelenggaraan TI.

c. Kebijakan, Standar, dan Prosedur

   Bank menetapkan kebijakan, standar, dan prosedur untuk seluruh penyelenggaraan TI.

   1) Kebijakan

      Kebijakan merupakan ketentuan atau prinsip yang menggambarkan komitmen, atau rencana Bank terhadap suatu masalah tertentu yang dinyatakan secara formal, dan menjadi landasan kerja bagi Bank.

   2) Standar

      Standar merupakan seperangkat aturan teknis yang harus dipatuhi dalam rangka menerapkan suatu kerangka kerja dan tata kelola TI (dapat berasal dari internal atau eksternal). Standar menetapkan persyaratan atau ukuran tertentu yang dapat digunakan sebagai acuan bagi Bank dalam menyelenggarakan TI.

      a) standar internal antara lain standar aplikasi desktop, standar konfigurasi komputer, dan standar penomoran dokumen.

      b) standar eksternal antara lain *International Organization for Standardization* (ISO), Standar

Nasional Indonesia (SNI), atau standar lain terkait penyelenggaraan TI.

3) Prosedur
Prosedur merupakan urutan kegiatan dari suatu proses penyelenggaraan TI yang melibatkan satu atau beberapa unit dan/atau fungsi dalam Bank.

Sesuai dengan Pasal 3 ayat (3) POJK PTI, kebijakan, standar, dan prosedur diterapkan oleh Bank secara konsisten dan berkesinambungan. Di samping itu, Bank wajib melakukan kaji ulang dan penginian kebijakan, standar, dan prosedur secara berkala sesuai dengan Pasal 3 ayat (4) POJK PTI.

Bank menetapkan jangka waktu kaji ulang dan penginian kebijakan, standar, dan prosedur sesuai dengan kebutuhan Bank dengan mempertimbangkan kondisi internal maupun eksternal Bank. Penetapan jangka waktu kaji ulang dan penginian kebijakan, standar, dan prosedur disusun Bank dalam suatu kebijakan tertulis.

Contoh:

Bank "X" menetapkan jangka waktu kaji ulang dan penginian untuk:

1) kebijakan setiap 5 (lima) tahun sekali;
2) standar setiap 2 (dua) tahun sekali; dan
3) prosedur setiap 1 (satu) tahun sekali.

d. Kebutuhan dan Alur Informasi Pendukung Proses Bisnis

Setiap keputusan, arahan, pemantauan, dan evaluasi dalam sistem tata kelola selalu membutuhkan informasi yang akurat, relevan, dan tepat waktu. Bank perlu memastikan bahwa informasi yang tersedia telah relevan, akurat, tepat waktu, aman, dan dapat ditindaklanjuti sesuai dengan kebutuhan Bank untuk mendukung proses bisnis Bank. Oleh karena itu, Bank perlu memastikan tersedianya Sistem Informasi Manajemen (SIM) yang dapat menghasilkan informasi yang diperlukan dalam rangka mendukung peran dan fungsi manajemen secara efektif. SIM yang dimiliki Bank harus dapat:

1) memfasilitasi pengelolaan operasional bisnis Bank termasuk pelayanan kepada nasabah;
2) mendokumentasikan dan mengumpulkan informasi secara objektif;
3) mendistribusikan data atau informasi ke berbagai satuan kerja yang sesuai, baik dari sisi jenis informasi, kualitas dan kuantitas informasi, maupun frekuensi dan waktu pengiriman laporan yang dibutuhkan;
4) meningkatkan efektivitas dan efisiensi komunikasi di Bank;
5) membantu Bank meningkatkan kepatuhan terhadap ketentuan peraturan perundang-undangan; dan
6) mendukung proses penilaian kinerja seluruh satuan kerja.

e. SDM Pendukung

Bank perlu memetakan, merencanakan, dan menetapkan jumlah, kompetensi dan keahlian SDM yang sesuai dalam penyelenggaraan TI. Pengembangan kompetensi dan keahlian SDM milik Bank, seperti penyelenggaraan pelatihan atau sertifikasi, perlu dilakukan agar SDM milik Bank dapat mendukung keberhasilan penerapan tata kelola TI. Termasuk dalam hal ini strategi dan persyaratan rekrutmen SDM Bank.

f. Budaya TI
Budaya TI merupakan nilai dan etika yang berlaku bagi pegawai sebagai individu maupun Bank sebagai organisasi, yang sesuai dengan tujuan pencapaian tata kelola TI. Bank menerapkan budaya TI pada seluruh unit dan/atau fungsi Bank. Budaya TI antara lain budaya inovasi dan budaya kolaborasi.

g. Infrastruktur dan Aplikasi
Bank memastikan tersedianya infrastruktur dan aplikasi yang diselenggarakan dengan memperhatikan tata kelola TI.

B. Peran dan Tanggung Jawab

Sesuai Pasal 4 POJK PTI, Bank wajib menetapkan wewenang dan tanggung jawab yang jelas dari Direksi, Dewan Komisaris, dan pejabat pada setiap jenjang jabatan yang terkait dengan penerapan tata kelola TI.

Keberhasilan penerapan tata kelola TI sangat tergantung pada komitmen dari Direksi, Dewan Komisaris, komite pengarah TI dan seluruh unit kerja di Bank, baik penyelenggara maupun pengguna TI. Penerapan tata kelola TI dilakukan melalui penyelarasan Rencana Strategis TI (RSTI) dengan rencana korporasi Bank, serta optimalisasi pengelolaan sumber daya, pemanfaatan TI, pengukuran kinerja, dan penerapan manajemen risiko yang efektif.

Perwujudan dari komitmen Direksi dan Dewan Komisaris yaitu dalam bentuk pengawasan aktif Direksi dan Dewan Komisaris terhadap tata kelola TI sebagaimana telah diatur dalam Pasal 5 dan Pasal 6 POJK PTI, serta terdapatnya peran aktif dari komite pengarah TI dalam memberikan rekomendasi terkait penyelenggaraan TI sebagaimana telah diatur dalam Pasal 7 POJK PTI. Sehubungan dengan hal itu, diperlukan kebijakan yang memuat peran dan tanggung jawab Direksi, Dewan Komisaris, dan komite pengarah TI dalam memastikan diterapkannya tata kelola TI.

1. Direksi

Selain wewenang dan tanggung jawab bagi Direksi sebagaimana diatur dalam Pasal 5 POJK PTI, wewenang dan tanggung jawab bagi Direksi juga dapat mencakup:

a. memastikan tersedianya SDM yang cukup dan kompeten sesuai dengan kebutuhan;
b. memastikan terdapat upaya peningkatan kompetensi SDM terkait penyelenggaraan TI, di antaranya melalui pendidikan atau pelatihan yang memadai dan program edukasi untuk meningkatkan kesadaran atas pengamanan informasi;
c. memastikan struktur organisasi manajemen proyek dari seluruh proyek terkait TI digunakan dengan maksimal;
d. memastikan bahwa Bank memiliki kontrak tertulis yang mengatur peran, hubungan, kewajiban, dan tanggung jawab dari semua pihak yang terikat kontrak tersebut, serta memiliki keyakinan bahwa kontrak tersebut merupakan perjanjian yang berkekuatan hukum dan melindungi kepentingan Bank, dalam hal Bank menggunakan jasa pihak lain;
e. menerapkan kepemimpinan yang berorientasi digital;
f. memastikan inisiatif digitalisasi atau transformasi digital yang dimuat dalam RSTI Bank sesuai dengan arah dan strategi Bank dalam rencana korporasi; dan
g. menerapkan program pengembangan budaya digital untuk mendukung transformasi digital.

Dalam menetapkan wewenang dan tanggung jawab bagi Direksi, Bank juga harus memperhatikan SEOJK Siber dan SEOJK DMAB.

2. Dewan Komisaris

Selain wewenang dan tanggung jawab bagi Dewan Komisaris sebagaimana diatur dalam Pasal 6 POJK PTI, wewenang dan tanggung jawab bagi Dewan Komisaris juga dapat mencakup:

a. mengevaluasi, mengarahkan, dan memantau kebijakan manajemen risiko di bidang TI dan kesesuaian penerapannya dengan karakteristik, kompleksitas, dan profil risiko Bank;
b. memberikan arahan perbaikan atas pelaksanaan kebijakan manajemen risiko di bidang TI;
c. melakukan evaluasi terhadap perencanaan dan pelaksanaan audit, memastikan audit dilaksanakan dengan frekuensi dan lingkup yang memadai, serta melakukan pemantauan atas tindak lanjut hasil audit yang terkait dengan sistem informasi;
d. melakukan evaluasi terhadap pengelolaan pengamanan yang andal dan efektif atas TI guna menjamin ketersediaan, kerahasiaan, dan keakuratan informasi;
e. mengevaluasi, mengarahkan, dan memantau kesesuaian, antara RSTI dengan arah dan strategi Bank dalam rencana korporasi;
f. mengevaluasi, mengarahkan, dan memantau penerapan kepemimpinan berorientasi digital; dan
g. mengevaluasi, mengarahkan, dan memantau penerapan program pengembangan budaya digital untuk mendukung transformasi digital.

Dalam menetapkan wewenang dan tanggung jawab bagi Dewan Komisaris, Bank juga harus memperhatikan SEOJK Siber dan SEOJK DMAB.

3. Komite Pengarah TI

Sesuai Pasal 7 POJK PTI, Bank wajib memiliki komite pengarah TI (*information technology steering committee*). Bagi Bank berupa Kantor Cabang dari Bank yang berkedudukan di Luar Negeri (KCBLN), fungsi komite pengarah TI dapat dilaksanakan oleh fungsi sejenis yang berada di kantor pusat atau kantor regional dari KCBLN. Komite pengarah TI perlu memiliki *information technology steering committee charter* yang mencantumkan wewenang dan tanggung jawab komite pengarah TI. Untuk dapat melaksanakan tugasnya secara efektif dan efisien, komite pengarah TI melakukan pertemuan secara berkala untuk membicarakan topik terkait dengan strategi TI, serta didokumentasikan dalam bentuk risalah rapat.

Wewenang dan tanggung jawab komite pengarah TI sebagaimana diatur dalam Pasal 7 POJK PTI adalah memberikan rekomendasi kepada Direksi yang paling sedikit terkait dengan:

a. RSTI yang sejalan dengan rencana korporasi Bank. Dalam memberikan rekomendasi, komite pengarah TI harus memperhatikan:
    1) peta jalan (*roadmap*) untuk mencapai kebutuhan TI yang mendukung strategi bisnis Bank. Peta jalan (*roadmap*) terdiri dari kondisi saat ini (*current state*), kondisi yang ingin dicapai (*future state*), dan langkah-langkah yang akan dilakukan untuk mencapai kondisi yang ingin dicapai;
    2) sumber daya yang dibutuhkan;
    3) manfaat yang akan diperoleh saat RSTI diterapkan; dan

4) kendala yang mungkin timbul dalam penerapan RSTI, dengan tetap mempertimbangkan faktor efektivitas dan efisiensi;

b. perumusan kebijakan, standar, dan prosedur TI yang utama, misalnya kebijakan pengamanan TI dan manajemen risiko terkait penggunaan TI di Bank;
c. kesesuaian antara rencana pengembangan TI dan RSTI. Komite pengarah TI juga menetapkan status prioritas rencana pengembangan TI yang bersifat kritikal dan berdampak signifikan terhadap kegiatan operasional Bank, misalnya pergantian *core banking system*, *server production*, dan topologi jaringan;
d. kesesuaian antara pelaksanaan pengembangan TI dengan rencana pengembangan TI yang disepakati antara lain melalui *project charter*. Komite pengarah TI harus melengkapi rekomendasi dengan hasil analisis dari pelaksanaan pengembangan TI yang utama sehingga memungkinkan Direksi mengambil keputusan secara efisien;
e. evaluasi atas efektivitas biaya TI terhadap pencapaian manfaat yang direncanakan, agar investasi TI dapat memberikan kontribusi terhadap pencapaian tujuan bisnis Bank;
f. pemantauan atas kinerja TI dan upaya peningkatan kinerja TI, misalnya deteksi infrastruktur TI yang sudah usang dan pengukuran efektivitas dan efisiensi penerapan kebijakan pengamanan TI;
g. upaya penyelesaian berbagai masalah terkait TI yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara TI secara efektif, efisien, dan tepat waktu; dan
h. kecukupan dan alokasi sumber daya terkait TI yang dimiliki Bank. Dalam hal sumber daya yang dimiliki tidak memadai dan Bank akan menggunakan jasa pihak lain dalam penyelenggaraan TI, komite pengarah TI harus memastikan Bank telah memiliki kebijakan dan prosedur yang dibutuhkan.

4. Pemimpin Satuan Kerja TI

Dalam rangka melakukan pengelolaan TI, Bank menetapkan wewenang dan tanggung jawab utama dari pejabat tertinggi yang memimpin satuan kerja TI mencakup paling sedikit:

a. merumuskan kebijakan, rencana, dan anggaran TI;
b. mengoordinasikan pengembangan TI Bank sesuai dengan rencana strategis yang telah ditetapkan;
c. menerapkan semua kebijakan, standar, dan prosedur TI serta rencana yang telah ditetapkan oleh Direksi;
d. memberikan dukungan pemberian jasa TI kepada satuan kerja pengguna TI untuk mencapai target bisnis secara responsif dan tepat waktu;
e. memastikan setiap informasi yang dimiliki oleh satuan kerja pengguna TI mendapatkan pelindungan yang baik terhadap semua gangguan yang dapat menyebabkan kerugian akibat bocornya data atau informasi penting;
f. memastikan kecukupan dan efektivitas kebijakan, prosedur TI, dan penerapan manajemen risiko untuk mengidentifikasi, mengukur, menilai, dan mengawasi risiko TI;
g. memastikan adanya pengawasan yang memadai dalam setiap pengembangan atau modifikasi sistem TI;
h. menyampaikan kepada Direksi mengenai laporan pelaksanaan TI secara berkala. Dalam hal diperlukan, juga dapat

mengusulkan tindakan untuk mengatasi kelemahan TI yang telah ditemukan;

i. menilai kinerja dari layanan TI di Bank, misalnya persentase berapa lama sistem mati (*downtime error*), pelanggaran keamanan, perkembangan proyek, dan penerapan perjanjian tingkat layanan (*Service Level Agreement*/SLA) antara satuan kerja TI dan satuan kerja pengguna atau PPJTI;
j. memastikan tindakan yang tepat telah dilakukan untuk memperbaiki temuan audit baik dari auditor intern maupun auditor ekstern atau berdasarkan laporan hasil pemeriksaan Otoritas Jasa Keuangan;
k. memastikan kecukupan SDM baik dalam penyelenggaraan TI maupun dalam penerapan manajemen risiko serta menjamin terpeliharanya SDM pada posisi TI yang bersifat kritikal dalam mendukung kelangsungan operasional dan pengembangan TI;
l. mengawasi implementasi anggaran (*budget*) TI seperti pengadaan dan pelatihan di bidang TI, dalam hal pejabat tertinggi satuan kerja TI adalah direktur;
m. bertanggung jawab terhadap penyusunan dan implementasi arsitektur TI serta rencana strategis lain yang mempengaruhi modal Bank secara signifikan, dalam hal pejabat tertinggi satuan kerja TI adalah direktur;
n. memastikan struktur organisasi manajemen proyek dari seluruh proyek terkait TI digunakan secara maksimal, dalam hal pejabat tertinggi satuan kerja TI adalah direktur; dan
o. memastikan bahwa kontrak tertulis antara Bank dengan PPJTI mencakup hal yang diatur bagi penggunaan pihak PPJTI.

Apabila satuan kerja TI tidak dipimpin oleh direktur TI maka peran dan tanggung jawab sebagaimana dimaksud dalam huruf l, huruf m, dan huruf n menjadi tanggung jawab direktur yang membawahkan satuan kerja TI.

C. Satuan Kerja TI

Sesuai Pasal 8 POJK PTI, Bank wajib memiliki satuan kerja penyelenggara TI yang bertanggung jawab atas pengelolaan TI. Pengelolaan TI paling sedikit berupa:

1. Perencanaan

Aktivitas utama dalam perencanaan yaitu menentukan rencana strategis dan arah penyelenggaraan TI, untuk dapat mendukung kebutuhan bisnis Bank. Dalam melakukan aktivitas perencanaan, satuan kerja TI harus paling sedikit:

a. menyusun RSTI yang diselaraskan dengan rencana korporasi Bank;
b. menyelaraskan rencana pengembangan TI agar sesuai RSTI yang telah ditetapkan dan tujuan bisnis dalam rencana korporasi Bank;
c. menyusun rencana investasi dalam penyelenggaraan TI, termasuk anggaran TI; dan
d. merencanakan strategi pengelolaan sumber daya TI.

2. Penyusunan atau Pengembangan

Aktivitas utama dalam penyusunan atau pengembangan yaitu memastikan pengembangan atas solusi TI dapat diimplementasikan secara efektif dan sesuai dengan kebutuhan Bank.

Dalam melakukan pengembangan TI, Bank memperhatikan proses:

a. Perencanaan, antara lain melakukan identifikasi dan analisis kebutuhan pengguna, dan pendefinisian kebutuhan pengguna;

b. Perancangan, pembuatan/konfigurasi (*build*) dan pengujian; dan
c. Implementasi dan reviu pascaimplementasi (*post-implementation review*).

Proses di atas dapat dilakukan sesuai dengan kebijakan serta metodologi pengembangan TI yang dilakukan oleh Bank. Bank juga harus menetapkan proses pengembangan TI dalam hal terdapat kondisi darurat (*emergency change*). Dalam hal pengembangan TI melibatkan PPJTI maka Bank harus memperhatikan pedoman mengenai penggunaan PPJTI sebagaimana diatur dalam Lampiran Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

Bank harus memiliki manajemen risiko yang memadai terhadap proses pengembangan TI agar dapat meminimalisasi berbagai risiko atau kerugian yang disebabkan adanya kesalahan (*error*), kecurangan (*fraud*), manipulasi data, penyalahgunaan sistem, atau ketidaktepatan fungsi layanan yang dikembangkan. Manajemen risiko terhadap proses pengembangan antara lain adanya kebijakan, standar, prosedur, serta proses identifikasi dan pengukuran risiko terhadap proses pengembangan TI.

Dalam melakukan pengembangan TI, Bank melakukan langkah pengendalian untuk menghasilkan integrasi sistem dan memastikan terjaganya kerahasiaan data, serta mendukung pencapaian tujuan Bank. Langkah pengendalian bertujuan untuk memastikan antara lain:

a. keakuratan dan berfungsinya sistem sesuai kebutuhan Bank;
b. kesesuaian sistem yang satu dengan sistem yang lain (interoperabilitas dan kompatibilitas);
c. ketersediaan dokumentasi atas pengembangan, perubahan dan pemeliharaan sistem;
d. terjaganya prinsip kerahasiaan, integritas dan ketersediaan;
e. kelangsungan operasional Bank, termasuk dalam hal Bank menggunakan PPJTI;
f. terdapat pemisahan lingkungan pengembangan dan operasional (*production environment*);
g. akuntabilitas tugas dan tanggung jawab dari seluruh pihak yang terlibat dalam pengembangan TI;
h. tersedianya rekam jejak audit (*audit trail*) dalam hal diperlukan untuk kepentingan pemeriksaan; dan
i. memiliki kode sumber (*source code*) atas perangkat lunak yang dikembangkan secara khusus untuk Bank yang bersangkutan (*proprietary*) sehingga kode sumber (*source code*) tersebut dapat diakses apabila diperlukan untuk kepentingan pemeriksaan dan penyidikan.

Proses pengembangan TI harus selalu di bawah kendali satuan kerja TI dan dikelola oleh manajemen proyek. Manajemen proyek dapat berbentuk tim kerja yang anggotanya paling sedikit berasal dari satuan kerja TI dan satuan kerja pengguna TI, yang bertugas untuk memastikan sistem telah dikembangkan dengan struktur yang baik dan telah mengakomodasi kebutuhan pengguna.

a. Kebijakan, Standar, dan Prosedur Pengembangan

Proses dalam pengembangan TI meliputi:

1) Tahap Perencanaan

Pada tahap perencanaan, Bank menerapkan langkah-langkah, antara lain:

a) identifikasi dan analisis kebutuhan pengguna untuk mendukung strategi bisnis Bank;

b) reviu dan persetujuan oleh Bank;
c) studi kelayakan proyek, yang antara lain berupa pertimbangan bisnis Bank, kebutuhan fungsional, rencana waktu pelaksanaan proyek, faktor-faktor yang mempengaruhi proyek serta analisis biaya dan manfaat;
d) persetujuan Bank atas dokumen studi kelayakan proyek;
e) penandatanganan dokumen studi kelayakan proyek oleh semua pihak yang terkait dalam pengembangan TI;
f) pengumpulan kebutuhan yang merupakan proses pengumpulan informasi, baik melalui metode wawancara, riset, dan/atau pengisian format dokumen atau formulir tertentu, mengenai tujuan pengembangan sistem, *output* yang diinginkan, kemampuan sistem dalam mengakomodasi kebutuhan proses bisnis dan mekanisme kerja sistem, serta prosedur penggunaan sistem;
g) analisis kebutuhan yang merupakan proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan;
h) penyusunan alur proses bisnis berdasarkan hasil analisis kebutuhan antara lain berupa *business process flow*, *use cases modeling* dan *data flow diagram*, yang dapat memperjelas pemahaman mengenai kebutuhan dan solusinya, baik bagi pengguna maupun pengembang sistem;
i) penentuan perkiraan umum dari waktu dan biaya pengembangan dari tiap kebutuhan dan kesesuaiannya dengan ketentuan peraturan perundang-undangan;
j) spesifikasi kebutuhan yang merupakan proses untuk mendeskripsikan fungsional sistem yang akan dikembangkan, spesifikasi proses atau prosedur dan sistem yang ada saat ini, baik dari segi perangkat lunak maupun perangkat keras pendukung serta desain pangkalan data (*database*). Spesifikasi kebutuhan harus lengkap, komprehensif, dapat diuji, konsisten, jelas, dan merinci kebutuhan *input*, proses, dan *output* yang dibutuhkan; dan
k) pengelolaan kebutuhan (*requirements management*) yang merupakan proses untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat pengembangan dilakukan oleh tim proyek.

2) Tahap Perancangan

Tahap perancangan terbagi menjadi 3 (tiga) langkah utama, yaitu:

a) Perancangan Sistem

Bank mengonversikan kebutuhan informasi, fungsi, dan infrastruktur yang teridentifikasi pada tahap perencanaan yang menjadi dasar pengembangan sistem. Dalam perancangan sistem, diperlukan suatu standar pengendalian aplikasi yang mencakup kebijakan dan prosedur terkait dengan aktivitas

pengguna dan pengendalian terintegrasi dalam sistem yang akan dikembangkan. Hal ini diperlukan untuk meningkatkan keamanan, integritas, dan keandalan sistem dengan memastikan informasi *input*, proses, dan *output* yang terotorisasi, akurat, lengkap dan aman. Bank perlu memperhatikan kesesuaian rancangan dengan arsitektur TI yang sudah dimiliki agar integrasi dan keberlangsungan antar sistem dapat terjaga.

b) Pemrograman

Bank mengonversikan spesifikasi desain menjadi program yang dapat dijalankan. Bank harus membuat kebijakan, standar, dan prosedur pemrograman. Selain itu, Bank harus menginikan rencana migrasi, implementasi, pelatihan pengguna akhir dan operator, serta dokumen manual pemeliharaan.

(1) Standar Pemrograman

Dalam standar pemrograman dijelaskan antara lain mengenai tanggung jawab *programmer* sistem. Manajer proyek harus memahami secara keseluruhan mengenai proses pemrograman untuk memastikan penerapan pengendalian pada aktivitas pemrograman telah memadai, antara lain:

(a) membatasi akses terhadap data, program, utilitas, dan sistem di luar tanggung jawab *programmer*; dan

(b) melakukan pengendalian versi sebagai metode yang secara sistematis menyimpan kronologis dari salinan program yang disempurnakan serta menjadi salah satu dokumentasi dalam penyelenggaraan pengembangan TI.

(2) Dokumentasi

(a) Bank harus mengelola dan memelihara dokumen yang detail untuk setiap sistem baik yang dikembangkan sendiri maupun produk atau perangkat lunak yang dibeli atau dikembangkan pihak lain yang mencakup:

i. deskripsi detail mengenai aplikasi;

ii. dokumentasi pemrograman berupa kode sumber (*source code*), dokumen yang dapat diunduh, dan tampilan dari sistem yang dikembangkan;

iii. standar format berbagai aspek yang digunakan terkait dengan sistem seperti pangkalan data (*database*), format tampilan, dan informasi;

iv. standar penamaan; dan

v. pedoman bagi operator dan pedoman bagi pengguna akhir dalam menjalankan fungsi pada sistem secara rinci, komprehensif, dan jelas.

(b) Dokumentasi harus dapat mengidentifikasikan standardisasi pengembangan, seperti narasi sistem, alur sistem, pengodean (*coding*) khusus sistem, dan pengendalian intern dalam dokumen aplikasi itu sendiri.

(c) Dalam hal produk atau perangkat lunak dibeli atau dikembangkan oleh pihak lain, Bank harus memastikan kaji ulang telah dilakukan sebelumnya baik secara internal maupun oleh pihak independen bahwa dokumentasi produk atau perangkat lunak telah sesuai dengan standar minimal dokumentasi Bank.

c) Uji Coba

Bank harus melaksanakan beberapa rangkaian uji coba untuk memastikan keakuratan dan berfungsinya sistem sesuai kebutuhan pengguna serta hubungan sistem tersebut dengan sistem lain yang telah digunakan oleh Bank. Seluruh koreksi dan modifikasi yang dilakukan selama uji coba harus didokumentasikan untuk menjaga integritas keseluruhan dokumentasi program. Bank harus melengkapi pedoman bagi pengguna dan pengelola serta menyiapkan rencana implementasi dan pelatihan.

Uji coba yang dapat dilakukan oleh Bank antara lain:

(1) *unit test*, yaitu uji coba yang dilakukan oleh pengembang atas fungsional setiap unit atau sub modul dari sistem yang telah selesai dikembangkan;

(2) *System Integration Test* (SIT), yaitu pengujian yang dilakukan oleh pengembang terhadap keseluruhan fungsional sistem setelah diintegrasikan menjadi satu kesatuan yang utuh;

(3) *stress test*, yaitu uji ketahanan yang dilakukan oleh pengembang terhadap kemampuan sistem dalam menangani proses atau transaksi dalam skala atau jumlah yang besar; dan

(4) *User Acceptance Test* (UAT), yaitu uji coba akhir yang dilakukan oleh pengguna akhir terhadap sistem yang telah selesai dikembangkan untuk menguji fungsionalitas keseluruhan sistem, apakah telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan. UAT oleh pengguna akhir dilakukan setelah pihak pengembang memberikan berita acara atas hasil pengujian SIT. Pada tahap ini audit intern dapat ikut melakukan pengujian dengan tetap menjaga tingkat independensi apabila audit intern perlu meyakini ketersediaan, kecukupan dan efektivitas pengendalian yang ada pada sistem. Jika hasil uji coba menunjukkan bahwa

sistem telah sesuai dengan kebutuhan pengguna dan standar pengamanan Bank maka harus dibuat suatu berita acara UAT yang disetujui pengguna.

3) Tahap Implementasi dan Kaji Ulang

Pada tahap ini Bank harus melakukan antara lain pemberitahuan jadwal implementasi, instalasi sistem yang telah disetujui ke dalam lingkungan operasional, dan pelatihan pada pengguna.

Hal yang harus diperhatikan antara lain:

a) pengecekan integritas program berupa pengendalian yang memadai terhadap konversi dari kode sumber (*source code*) ke *object code* yang akan diimplementasikan;
b) migrasi data dari sistem lama ke sistem baru;
c) pengecekan akurasi dan keamanan data hasil migrasi pada sistem baru;
d) kemungkinan diberlakukannya secara bersama (*parallel run*) antara sistem yang lama dengan yang baru, sampai dipastikan bahwa data pada sistem yang baru telah akurat dan andal;
e) Bank harus memastikan integritas data berupa keakuratan dan keandalan dari pangkalan data (*database*) termasuk data yang tersimpan di dalamnya;
f) perbaikan data dan referensi secara langsung (*patching data*) pada saat implementasi sebaiknya dihindari karena dapat mempengaruhi integritas data pada pangkalan data (*database*) di server produksi;
g) pengaturan penyimpanan kode sumber (*source code*) dan pangkalan data (*database*) dari sistem lama; dan
h) antisipasi adanya kelemahan sistem operasi, sistem yang dikembangkan, pangkalan data (*database*) dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti virus, *trojan horse*, *worms*, *spyware*, *Denial-of-Service* (DoS), *wardriving*, *spoofing* dan *logic bomb*, dengan menguji dan menerapkan pengendalian pengamanan atas sistem yang akan diimplementasikan.

Bank harus melakukan kaji ulang pascaimplementasi (*post-implementation review*) pada akhir proyek untuk mengetahui bahwa seluruh aktivitas dalam proyek telah dilaksanakan dan tujuan proyek telah tercapai. Efektivitas aktivitas manajemen proyek dilakukan dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek. Hasil analisis harus didokumentasikan untuk mendukung kebutuhan pelaporan terkait proyek.

Dalam hal pengembangan sistem juga melibatkan proses pengadaan maka perlu pula diperhatikan kesesuaian spesifikasi dengan kebutuhan Bank, pengaruh terhadap sistem yang telah ada, dukungan teknis purnajual, reputasi vendor, kelengkapan dokumentasi, *escrow agreement*, dan pelatihan.

Dalam proses pengadaan sistem, Bank juga harus memastikan bahwa:

1) pengadaan perangkat keras dan perangkat lunak telah melalui studi kelayakan proyek, mendapatkan persetujuan Bank, terdapat pendefinisian kebutuhan pengguna, memiliki pengendalian dan pengamanan sistem yang memadai, serta terdapat pengujian dan implementasi produk; dan
2) terdapat pembuktian bahwa aplikasi yang akan dibeli dari vendor dapat memenuhi kebutuhan Bank (*Proof of Concept*/PoC). Beberapa pendekatan yang dapat digunakan untuk tujuan pembuktian konsep tersebut antara lain:
   a) konsep dari vendor yang telah dibangun dalam bentuk purwarupa (*prototype*) telah melewati tahap pengujian oleh sekelompok kecil pengguna operasional yang meliputi beberapa jenis peran (*business role*);
   b) pembuktian konsep dapat dilakukan secara teknis terhadap seluruh aspek teknologi yang terlibat dalam aplikasi (*steel thread*);
   c) pembuktian teknologi (*proof of technology*) dapat dilakukan untuk memastikan teknologi yang akan diadopsi dapat mengatasi permasalahan teknis yang ada. Misalnya teknologi dimaksud dapat mengintegrasikan dua sistem yang berbeda atau dapat mencapai kinerja tertentu dengan konfigurasi yang telah ditetapkan. Proses pembuktian teknologi tidak perlu melibatkan pengguna operasional; dan
   d) implementasi dalam ruang lingkup yang lebih kecil dapat didahului dengan proyek percobaan (*pilot project*) dengan target akhir yang lebih terbatas. Pembatasan ruang lingkup dapat dilakukan dengan cara membatasi jumlah pengguna yang dapat mengakses sistem, jumlah proses bisnis, komponen organisasi dan pemangku kepentingan (*stakeholders*) yang terlibat, atau batasan lain yang dinilai layak. Tujuan proyek percobaan ini yaitu untuk menguji kinerja sistem sesuai harapan dengan membatasi risiko kerugian bagi Bank jika terdapat kegagalan sistem.

b. Manajemen Proyek dan Manajemen Perubahan dalam Pengembangan TI

Dalam melakukan pengembangan TI, Bank perlu melakukan manajemen proyek dengan memperhatikan, antara lain:

1) Bank memastikan kecukupan sumber daya untuk mencapai tujuan proyek, dengan memperhatikan ketepatan waktu, kesesuaian biaya, dan kualitas;
2) Bank harus memastikan kecukupan pelatihan dan kejelasan petunjuk penggunaan sistem informasi yang disusun;
3) Bank memastikan seluruh hasil (*deliverables*) pada setiap tahapan manajemen proyek harus didokumentasikan dengan baik; dan

4) Bank harus memiliki dokumentasi *project charter*, yang memuat paling sedikit:
   a) informasi proyek, antara lain kode, sponsor, dan manajer proyek;
   b) tujuan proyek, informasi latar belakang, dan strategi pengembangan;
   c) deskripsi tugas dan tanggung jawab utama dari tiap pihak dalam manajemen proyek;
   d) kriteria keberhasilan untuk masing-masing tahap pengembangan;
   e) identifikasi risiko proyek;
   f) mekanisme pemantauan pencapaian proyek;
   g) jadwal proyek; dan
   h) estimasi anggaran.

   Dalam hal terdapat perubahan yang berdampak signifikan terhadap pelaksanaan proyek maka Bank harus meninjau kembali perencanaan proyek tersebut.

3. Pengoperasian

Aktivitas utama dalam pengoperasian yaitu menjalankan layanan TI secara stabil, aman, dan berkelanjutan. Bank perlu menerapkan pengendalian yang memadai atas operasional TI agar Bank dapat meminimalkan risiko terganggunya kerahasiaan, integritas, dan ketersediaan informasi.

a. Pusat Data dan Pusat Pemulihan Bencana

Operasional TI pada penyelenggaraan Pusat Data (*Data Center*/DC) dan Pusat Pemulihan Bencana (*Disaster Recovery Center*/DRC) harus dapat menjamin kelangsungan usaha Bank.

1) Aktivitas Operasional Pusat Data

   Kebijakan, standar, dan prosedur serta sistem yang diterapkan dalam aktivitas operasional Pusat Data mencakup aktivitas rutin maupun tidak rutin. Aktivitas yang terkait dengan operasional Pusat Data antara lain:
   a) penjadwalan tugas (*shifting*);
   b) pelaksanaan tugas rutin sesuai kewenangan;
   c) proses rekam cadang (*backup*) baik *onsite* maupun *offsite*, *restore*, unduh (*download*), dan unggah (*upload*) untuk pangkalan data (*database*); dan
   d) pemantauan perangkat keras dan perangkat lunak.

2) Pengendalian Akses Fisik Pusat Data

   Pengendalian akses fisik ke Pusat Data antara lain:
   a) pintu Pusat Data harus selalu terkunci dan dilengkapi dengan kartu akses dan/atau *biometric device*;
   b) ruang Pusat Data tidak boleh diberi label atau papan petunjuk (*signing board*) agar orang tidak mudah mengenali; dan
   c) Bank harus memiliki *log-book* untuk mencatat tamu yang memasuki Pusat Data.

3) Pengendalian Lingkungan Pusat Data

   Pengendalian Lingkungan Pusat Data antara lain:
   a) pengawasan dan pemantauan faktor lingkungan dan fasilitas Pusat Data, antara lain mencakup sumber listrik, api, air, suhu, dan kelembaban udara. Pengendalian lingkungan yang dapat diterapkan antara lain penggunaan *Uninterruptible Power Supply*

(UPS), lantai yang ditinggikan (*raised floor*), pengaturan suhu dan kelembaban udara dengan pemanfaatan *Air Conditioner* (AC), termometer dan higrometer, pendeteksi asap dan/atau api, sistem pemadaman api, dan kamera *Closed-Circuit Television* (CCTV);

b) ketersediaan sumber listrik yang cukup, stabil, serta sumber listrik alternatif untuk mengantisipasi tidak tersedianya pasokan listrik dari sumber listrik utama. Untuk mengantisipasi putusnya arus listrik sewaktu-waktu, Bank perlu memastikan pengatur voltase listrik, UPS, dan generator listrik dapat bekerja dengan baik pada saat diperlukan. Bank juga harus menggunakan metode pemindahan secara otomatis (*automatic switching*) apabila terjadi gangguan pada salah satu sumber listrik untuk menjaga pasokan listrik yang sesuai dengan kebutuhan peralatan;

c) memastikan Pusat Data memiliki detektor api dan asap serta pipa pembuangan air. Bank juga harus menyediakan sistem pemadam api yang memadai, baik yang dapat beroperasi secara otomatis maupun dioperasikan secara manual. Zat pemadam api dan sistem yang digunakan harus memperhatikan keamanan terhadap peralatan dan petugas pelaksana di dalam Pusat Data;

d) menggunakan lantai yang ditinggikan (*raised floor*) untuk mengamankan sistem perkabelan dan menghindari efek *grounding* di Pusat Data; dan

e) menginventarisasi perangkat pendukung Pusat Data.

b. Kebijakan Pengelolaan Konfigurasi Perangkat Keras dan Perangkat Lunak

Bank harus menetapkan prosedur terkait:

1) proses instalasi perangkat keras dan perangkat lunak;
2) pengaturan parameter (*hardening*) perangkat keras dan perangkat lunak; dan
3) inventarisasi dan penginian informasi perangkat keras, perangkat lunak, infrastruktur jaringan, media penyimpan, dan perangkat pendukung lain yang terdapat di Pusat Data. Inventarisasi yang dilakukan meliputi:
   a) Perangkat keras
      Inventarisasi perangkat keras harus dilakukan secara menyeluruh termasuk inventarisasi terhadap perangkat keras milik pihak lain yang berada di Bank. Informasi penting yang harus dicakup dalam inventarisasi perangkat keras antara lain nama vendor, model, tanggal pembelian, tanggal instalasi, kapasitas *processor*, memori utama, kapasitas penyimpanan, sistem operasi, fungsi, dan lokasi.
   b) Perangkat lunak
      Bank harus menginventarisasi informasi mengenai nama dan jenis perangkat lunak seperti sistem operasi, sistem aplikasi, atau sistem utilitas. Informasi lain yang harus dicakup dalam inventarisasi perangkat lunak, antara lain nama vendor, tanggal instalasi, nomor versi dan keluaran

(*release*), pemilik perangkat lunak, *setting parameter* dan *service* yang aktif, jumlah lisensi yang dimiliki, jumlah perangkat lunak yang di-*install*, dan jumlah pengguna.

c) Infrastruktur jaringan
Bank harus mendokumentasikan secara lengkap informasi terkait konfigurasi dari setiap infrastruktur jaringan. Cakupan informasi dalam dokumentasi konfigurasi jaringan antara lain:
(1) diagram dan konfigurasi perangkat jaringan dan perangkat pengamanan jaringan;
(2) daftar koneksi internal dan eksternal Bank;
(3) daftar dan spesifikasi peralatan jaringan seperti *switch*, *router*, *hub*, *gateway*, dan *firewall*; dan
(4) daftar vendor telekomunikasi.

d) Media penyimpan
Informasi yang diperlukan dalam inventarisasi media penyimpan antara lain jenis dan kapasitas, lokasi penyimpanan baik *onsite* maupun *offsite*, tipe dan klasifikasi data yang disimpan, serta frekuensi dan masa retensi rekam cadang (*backup*).

c. Kebijakan Pemeliharaan Perangkat Keras dan Perangkat Lunak

Pemeliharaan preventif secara berkala terhadap perangkat TI dilakukan untuk meminimalisasi kegagalan pengoperasian perangkat TI serta mendeteksi potensi permasalahan secara dini.

Bank harus menetapkan metodologi pemeliharaan yang sesuai dengan karakteristik dan risiko dari sistem yang ada. Pemeliharaan dilaksanakan sebagai jaminan bagi pengguna agar dapat terus menjalankan sistem sesuai dengan kebutuhan terkini. Tahap pemeliharaan memperhatikan aspek antara lain:

1) Perubahan Sistem TI
Dalam hal terjadi penggabungan, peleburan, pengambilalihan, integrasi, dan konversi Bank yang memerlukan pengintegrasian sistem yang digunakan oleh Bank yang terlibat dalam penggabungan, peleburan, pengambilalihan, integrasi, dan konversi maka perlu dilakukan proses perubahan sistem TI. Dalam proses ini dilakukan modifikasi atau perubahan besar pada sistem yang ada dan pengembangan sistem baru apabila diperlukan. Proses yang terstruktur seperti manajemen proyek dan siklus pengembangan sistem tetap harus diterapkan.
Mengingat kompleksitas sistem di masing-masing Bank yang terlibat penggabungan, peleburan, pengambilalihan, integrasi, dan konversi maka diperlukan analisis secara komprehensif terhadap dampak perubahan pada kegiatan operasional Bank khususnya pemrosesan transaksi. Agar proses perubahan berlangsung secara efektif, Bank perlu mengantisipasi peningkatan permintaan untuk *balancing*, *reconcilement*, *exception handling*, dukungan pengguna dan nasabah, penyelesaian masalah, keterhubungan jaringan, dan sistem administrasi.

2) Pemeliharaan Dokumentasi
Standar dokumentasi harus mengidentifikasikan dokumen utama dan dokumen detail yang telah disetujui dan sesuai format yang dibutuhkan. Dokumentasi tersebut harus berisi semua perubahan yang terjadi pada sistem baik dari perangkat lunak, perangkat keras, dan jaringan, serta konfigurasi sesuai dengan standar yang ditentukan.
Dokumentasi terkait sistem hanya dapat diakses oleh personel Bank yang berhak dan/atau memiliki kewenangan untuk mengadministrasikan dokumentasi tersebut. Bank harus memiliki lokasi penyimpanan khusus dokumentasi baik yang berupa *hardcopy* maupun *softcopy*, termasuk lokasi yang akan digunakan untuk kondisi darurat.

d. Kebijakan Manajemen Perubahan (*Change Management*)

Manajemen perubahan merupakan prosedur yang mengatur penambahan, penggantian, maupun penghapusan objek di lingkungan operasional. Objek dimaksud dapat berupa data, program, menu, aplikasi, perangkat komputer, perangkat jaringan, dan proses. Bank harus memiliki kebijakan, standar, dan prosedur manajemen perubahan yang mencakup paling sedikit permintaan, analisis, persetujuan perubahan, dan instalasi perubahan termasuk pemindahan perangkat keras dan perangkat lunak dari lingkungan pengujian ke lingkungan operasional.

Proses manajemen perubahan terdiri atas paling sedikit:

1) peninjauan ulang sebelum modifikasi dan otorisasi;
2) pengujian sebelum modifikasi dalam lingkungan pengujian yang terpisah;
3) prosedur rekam cadang (*backup*) data dan kode sumber (*source code*) sebelum modifikasi; dan
4) dokumentasi yang diperlukan, antara lain:
   a) penjelasan dari modifikasi;
   b) tanggal dan waktu modifikasi dilakukan;
   c) identifikasi sistem, pangkalan data (*database*), dan satuan kerja yang terpengaruh;
   d) kebutuhan sumber daya;
   e) pertimbangan potensi keamanan dan keandalan modifikasi sistem;
   f) prosedur implementasi; dan
   g) evaluasi setelah modifikasi.

Manajemen perubahan harus memperhatikan:

1) Pengendalian perubahan
Ketergantungan antar aplikasi yang digunakan pada berbagai satuan kerja memerlukan penyelenggaraan TI yang terintegrasi. Oleh karena itu, semua perubahan harus melalui fungsi pengawasan dalam manajemen perubahan yang terkoordinasi dan melibatkan perwakilan dari satuan kerja bisnis, unit penyelenggara TI, keamanan informasi, dan audit intern. Prosedur instalasi perubahan harus memperhatikan kelangsungan operasional pada lingkungan operasional, pengawasan, dan pengaturan pengamanan sistem informasi. Standar minimal yang diatur harus mencakup risiko, pengujian, otorisasi dan

persetujuan, waktu implementasi, validasi setelah penginstalan, dan *back-out* atau *recovery*.

2) *Patch managements*
Dalam manajemen perubahan, Bank harus memiliki dokumentasi yang lengkap tentang instalasi *patch* yang dilakukan. Selain itu, Bank harus memastikan bahwa Bank menggunakan versi perangkat lunak yang telah teruji. Bank juga harus memiliki informasi terkini mengenai perbaikan produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan.

3) Migrasi data
Migrasi data terjadi jika terdapat perubahan besar pada sistem aplikasi atau terjadi penggabungan data dari beberapa sistem yang berbeda. Dalam hal terdapat migrasi data, Bank perlu memiliki kebijakan, standar, dan prosedur mengenai penanganan migrasi data. Tahap-tahap yang perlu dilalui dalam melakukan migrasi data dimulai dari rencana strategis, manajemen proyek, manajemen perubahan, pengujian, rencana kontinjensi, rekam cadang (*backup*), manajemen vendor, dan *post-implementation review*.

e. Kebijakan Penanganan Kejadian atau Permasalahan

Prosedur penanganan kejadian atau permasalahan yang baik dibutuhkan Bank untuk menghadapi risiko finansial, operasional, dan reputasi dari permasalahan yang timbul. Prosedur penanganan kejadian atau permasalahan harus mencakup seluruh infrastruktur TI antara lain perangkat keras, sistem operasi, sistem aplikasi, perangkat jaringan, dan perangkat keamanan. Prosedur penanganan kejadian atau permasalahan memperhatikan kritikalitas dan urgensi dari kejadian atau permasalahan.

Bank harus memelihara sarana yang diperlukan untuk menangani permasalahan antara lain:

1) Pengelolaan *Helpdesk*
Bank harus memiliki fungsi *helpdesk* agar Bank dapat menanggapi dan menangani permasalahan yang dihadapi oleh seluruh pengguna di Bank dengan segera.
Hal yang perlu diperhatikan dalam fungsi *helpdesk* antara lain:
   a) tersedianya dokumentasi permasalahan yang lengkap, mencakup data pengguna, penjelasan masalah, dampak pada sistem, skala prioritas, status resolusi saat ini, pihak yang bertanggung jawab terhadap resolusi, akar permasalahan jika teridentifikasi, target waktu resolusi, dan *field* komentar untuk mencatat kontak pengguna dan informasi relevan lain; dan
   b) tersedianya sistem *helpdesk* yang dapat membantu staf *helpdesk* tentang alternatif solusi permasalahan yang umum terjadi, yang dikinikan secara berkala.

2) Pengelolaan *Privilege Access*
Privilege access merupakan akun atau *user* yang memiliki hak akses khusus terhadap sistem dan jaringan dalam rangka penanganan kejadian atau permasalahan. Bank menetapkan prosedur pengelolaan *privilege access* agar

penggunaannya tidak disalahgunakan. Prosedur tersebut antara lain mengatur:

a) penetapan pihak yang memiliki hak *privilege access* termasuk penerapan *dual custody* (pemecahan *password* kepada lebih dari 1 (satu) orang);
b) prosedur penyimpanan *password privilege access*;
c) prosedur *break ID privilege access* pada keadaan darurat;
d) prosedur penggantian *password privilege access* setelah digunakan; dan
e) pendokumentasian penggunaan *privilege access* dalam bentuk berita acara atau dalam bentuk lain.

f. Pengelolaan Pangkalan Data (*Database*)

Kegagalan dalam mengelola dan mengamankan pangkalan data (*database*) dapat mengakibatkan perubahan, penghancuran, atau pengungkapan informasi yang sensitif oleh pengguna secara sengaja maupun tidak sengaja atau oleh pihak lain yang tidak berhak.

Pengungkapan tanpa izin terhadap informasi yang rahasia dapat mengakibatkan risiko reputasi, hukum, dan operasional serta dapat menyebabkan kerugian finansial.

Bank perlu memiliki klasifikasi sensitivitas atas informasi yang disimpan pada pangkalan data (*database*) sebagai dasar untuk melakukan penerapan pengamanan yang sesuai. Pangkalan data (*database*) yang menyimpan informasi rahasia membutuhkan pengendalian yang lebih ketat dibandingkan pangkalan data (*database*) yang menyimpan informasi yang tidak sensitif. Untuk itu, Bank memiliki fungsi *Database Administrator* (DBA) yang bertanggung jawab terhadap pengelolaan pangkalan data (*database*) Bank. Prosedur yang dimiliki Bank terkait pangkalan data (*database*) antara lain pengaksesan, pemeliharaan, penanganan permasalahan, dan administrasi pangkalan data (*database*).

g. Pengendalian Pertukaran Informasi (*Exchange of Information*)

Pengiriman informasi secara daring (*online*) maupun melalui media penyimpan (seperti *tape* dan *disk*) harus dikelola secara memadai oleh Bank untuk mencegah risiko terkait pengamanan informasi. Bank harus memiliki prosedur pengelolaan transmisi informasi secara fisik dan *logic* antara lain:

1) permintaan dan pemberian informasi oleh pihak internal dan eksternal; dan
2) pengiriman informasi melalui berbagai media, seperti *hardcopy*, *tape*, *disk*, *email*, pos, dan internet.

Bank harus mempertimbangkan pemisahan segmen *Wide Area Network* (WAN) dan *Local Area Network* (LAN) dengan perangkat pengamanan seperti *firewall* yang membatasi akses dan lalu lintas keluar masuknya data, sesuai dengan kompleksitas TI Bank.

h. Pengelolaan Repositori

Pengelola repositori bertanggung jawab untuk menginventarisasi dan menyimpan informasi terkait seluruh aset TI, perangkat lunak dan data yang tersimpan dalam berbagai media. Pengelola repositori memastikan informasi dan aset TI terdokumentasi dan dapat diakses dengan benar untuk

mendukung proses layanan TI. Di samping itu, pengelola repositori juga menyimpan salinan dari seluruh kebijakan dan prosedur seperti *run book manual* terkait Pusat Data. Adapun prosedur yang harus ditetapkan antara lain:

1) pengamanan akses ke data di repositori;
2) penanganan media penyimpan data (untuk pangkalan data (*database*) dan audit *journal*);
3) masa retensi media penyimpan data;
4) pengujian media penyimpan data; dan
5) keluar dan masuk media penyimpan data dari dan ke repositori.

Dalam membuat kebijakan, standar, dan prosedur untuk pengelolaan repositori Bank harus memperhatikan kecukupan prosedur penyimpanan (*storage*), rekam cadang (*back-up*), dan pemusnahan (*disposal*) media. Rekam cadang (*back-up*) data maupun program harus selalu dikinikan agar Bank dapat memastikan kemampuannya untuk memulihkan sistem, aplikasi, dan data pada saat terjadi bencana atau gangguan lain.

i. Pemusnahan (*Disposal*) Perangkat Keras dan Perangkat Lunak

Setiap aset TI yang sudah tidak digunakan lagi dalam kegiatan operasional dan berdasarkan pertimbangan Bank diyakini tidak akan diperlukan dan tidak akan dipelihara lagi maka aset tersebut akan memasuki tahap pemusnahan (*disposal*). Hal ini dilakukan untuk memastikan penggunaan aset TI sistem yang paling akurat dan terkini yang digunakan dalam kegiatan operasional serta menghindari penyalahgunaan oleh pihak tidak berwenang.

Pemusnahan meliputi penghapusan perangkat lunak, perangkat keras, dan data yang sudah tidak digunakan lagi atau yang masa retensinya telah habis. Sebagai contoh, untuk penanganan perangkat lunak, kode sumber (*source code*) versi lama yang sudah tidak dipakai lagi harus disimpan dengan informasi yang jelas mengenai tanggal, waktu, dan informasi lain ketika digantikan dengan kode sumber (*source code*) versi terbaru.

Hal yang perlu diperhatikan pada tahap pemusnahan:

1) masa retensi dari data atau *end of life* dari aset TI;
2) memastikan seluruh data yang bersifat sensitif telah dihapus/dimusnahkan, sesuai dengan masa retensi;
3) melakukan penyesuaian atau penghapusan terhadap akses/konfigurasi aset TI yang tidak gunakan;
4) dokumentasi informasi perpindahan aset TI yang akan dilakukan pemusnahan (*disposal*);
5) menerapkan metode pemusnahan (*disposal*) yang sesuai dengan klasifikasi aset TI, seperti *degaussing* atau *shredding*; dan
6) persetujuan yang memadai untuk melakukan pemusnahan (*disposal*).

4. Pemantauan

Aktivitas utama dalam pemantauan yaitu untuk mengukur, mengevaluasi, dan memastikan bahwa TI berjalan sesuai tujuan, kebijakan, dan regulasi. Termasuk mengidentifikasi hal yang dapat ditingkatkan dan dikembangkan dalam rangka pengelolaan TI.

BAB III
ARSITEKTUR TI BANK

A. Arsitektur TI

Arsitektur TI merupakan dokumentasi strategis atas sumber daya TI Bank yang terorganisasi dan terintegrasi untuk mencapai dan mendukung tujuan bisnis Bank. Arsitektur TI mencakup sumber daya TI berupa data, aplikasi, dan teknologi yang digunakan oleh Bank dalam mendukung bisnisnya. Arsitektur TI merupakan *living document* yang dapat disesuaikan sesuai dengan kebutuhan dan perkembangan bisnis Bank.

1. Faktor Pertimbangan dalam Penyusunan Arsitektur TI

Sebagaimana diatur dalam Pasal 11 ayat (2) POJK PTI, penyusunan arsitektur TI perlu mempertimbangkan faktor paling sedikit:

a. Visi dan Misi Bank

Visi dan misi Bank menggambarkan tujuan yang ingin dicapai oleh Bank dalam jangka panjang serta langkah dan/atau upaya yang diperlukan untuk mencapai tujuan dimaksud. Pengembangan TI harus sejalan dengan visi dan misi Bank sehingga dapat mendukung bisnis dan operasional Bank dengan baik.

b. Rencana Korporasi Bank

Rencana korporasi Bank merupakan rencana strategis jangka Panjang untuk 5 (lima) tahun secara menyeluruh, yang berisi rumusan arah untuk mencapai tujuan Bank.

c. Proses dan Kapabilitas Bisnis Bank

Proses bisnis merupakan serangkaian aktivitas yang saling terkait dan menghasilkan nilai dalam rangka mencapai tujuan bisnis. Sedangkan, kapabilitas bisnis merupakan kemampuan yang perlu dimiliki untuk melakukan proses bisnis sehingga mencapai tujuan bisnis.

d. Tata Kelola TI

Tata kelola TI merupakan tata kelola TI sebagaimana dicantumkan pada Bab II Tata Kelola TI Bank.

e. Prinsip Pengelolaan Data, Aplikasi, dan Teknologi Bank

Prinsip pengelolaan data, aplikasi, dan teknologi Bank merupakan pedoman umum yang mendasari penggunaan dan penerapan seluruh sumber daya dan aset TI di Bank.

f. Ukuran dan Kompleksitas Bisnis Bank

Penyusunan arsitektur TI perlu disesuaikan dengan ukuran dan kompleksitas bisnis Bank. Bank dengan kompleksitas bisnis yang tinggi memerlukan arsitektur TI yang lebih detail agar Bank dapat mengelola kompleksitas TI yang dimiliki dengan baik.

g. Kemampuan Permodalan Bank

Kemampuan permodalan Bank menjadi bahan pertimbangan dalam proses alokasi biaya TI dalam bentuk biaya investasi maupun biaya operasional.

h. Standar yang Berlaku Secara Nasional Maupun Internasional

Praktik atau standar yang berlaku secara nasional maupun internasional menjadi pertimbangan dalam penyusunan arsitektur TI.

i. Ketentuan Peraturan Perundang-Undangan

Penyusunan arsitektur TI dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Selain faktor-faktor tersebut di atas, Bank dapat mempertimbangkan faktor lain sesuai dengan karakteristik bisnis Bank.

2. Penyusunan Arsitektur TI

Sebagaimana diatur dalam Pasal 11 ayat (3) POJK PTI, proses penyusunan arsitektur TI Bank meliputi tahapan perencanaan, desain, implementasi, dan kontrol. Dalam menyusun arsitektur TI, Bank perlu memiliki kebijakan dan prosedur penyusunan arsitektur TI. Arsitektur TI yang disusun menggambarkan kondisi saat ini (*current state*) dan kondisi yang ingin dicapai oleh Bank (*future state*). Selain itu, Bank perlu menginikan Arsitektur TI secara berkala maupun sewaktu-waktu apabila diperlukan.

a. Tahap Perencanaan

Pada tahap perencanaan, Bank melakukan penentuan prinsip arsitektur serta penetapan peran dan tanggung jawab. Penentuan prinsip arsitektur bertujuan agar terdapat keselarasan arah kebijakan pengembangan TI pada setiap unit atau fungsi di Bank. Selanjutnya, Bank juga perlu memastikan terdapat pihak yang bertanggung jawab atas penyusunan arsitektur TI Bank.

1) Penentuan Prinsip Arsitektur

Prinsip Arsitektur mendefinisikan aturan dan pedoman umum yang mendasari penggunaan dan penerapan seluruh sumber daya dan aset TI di Bank. Prinsip-prinsip ini mencerminkan suatu tingkat kesepahaman di antara unit kerja dan memberikan dasar dalam pengambilan keputusan terkait TI. Dengan demikian, kebijakan pengembangan TI Bank tetap sesuai dengan tujuan bisnis Bank.

Beberapa prinsip yang dapat diacu dalam penyusunan arsitektur, antara lain:

No.	Prinsip	Penjelasan
1.	Manajemen Informasi adalah Tanggung Jawab Setiap Pihak	Setiap unit bisnis berpartisipasi dalam pengambilan keputusan terkait manajemen informasi yang diperlukan untuk mencapai tujuan bisnis.
2.	Keberlangsungan Bisnis	Operasional Bank tetap harus dapat berjalan dalam kondisi gangguan sistem.
3.	Aplikasi untuk Penggunaan Bersama	Pengembangan aplikasi yang dapat digunakan secara bersama di seluruh unit bisnis Bank lebih diutamakan dibandingkan pengembangan aplikasi lain yang serupa atau duplikat yang hanya digunakan oleh unit bisnis tertentu.
4.	Kepatuhan terhadap Hukum dan Regulasi yang Berlaku	Proses manajemen informasi pada Bank patuh terhadap hukum dan regulasi yang relevan.
5.	Data merupakan Aset	Data merupakan aset yang bernilai bagi Bank, sehingga perlu dikelola dengan baik.

6.	Kemudahan Akses Data	Data dapat diakses oleh pengguna untuk menjalankan fungsi sesuai kewenangan.
7.	Keamanan Data	Data dilindungi dari penggunaan, perubahan, dan pengungkapan yang tidak sah.
8.	Perubahan yang Berdasarkan Kebutuhan	Perubahan pada aplikasi dan teknologi hanya dilakukan sebagai respons dari kebutuhan bisnis.
9.	Interoperabilitas	Perangkat lunak dan keras yang dimiliki harus memenuhi standar yang mengedepankan interoperabilitas data, aplikasi, dan teknologi.

Sesuai dengan kebutuhan dan kompleksitas bisnis, Bank dapat menyesuaikan prinsip arsitektur sebagaimana di atas. Bank perlu melengkapi prinsip yang diacu dengan penjelasan lebih lanjut, pertimbangan atas prinsip, implikasi penerapan, serta contoh penerapan prinsip, sesuai dengan karakteristik Bank.

2) Penetapan Peran dan Tanggung Jawab

Bank menetapkan unit atau fungsi yang bertanggung jawab terhadap penyusunan arsitektur TI. Unit atau fungsi tersebut berkoordinasi dengan satuan kerja terkait dalam penyusunan arsitektur TI untuk memastikan kesesuaian dengan tujuan bisnis.

Unit atau fungsi yang bertanggung jawab terhadap penyusunan arsitektur TI memiliki tugas pokok, antara lain:

a) bertanggung jawab untuk merancang arsitektur TI guna mencapai tujuan bisnis dan rencana strategis Bank;
b) memastikan bahwa arsitektur TI dapat memberikan gambaran secara lengkap mengenai kondisi TI Bank terkini dan yang ingin dicapai untuk mendukung operasional unit Bank secara terintegrasi;
c) mengomunikasikan arsitektur TI dalam mencapai tujuan bisnis kepada manajemen Bank;
d) meninjau infrastruktur dan aktivitas TI yang ada dan bekerja sama dengan unit terkait untuk menentukan kapabilitas yang dibutuhkan oleh sistem TI untuk memberikan produk atau layanan baru; dan
e) bekerja sama dengan unit terkait untuk mengevaluasi implikasi perencanaan strategis antara lain perubahan signifikan pada arsitektur TI terhadap lanskap teknologi Bank.

b. Tahap Desain

Pada tahap desain atau perancangan, Bank merancang arsitektur TI yang meliputi arsitektur data, arsitektur aplikasi, dan arsitektur teknologi. Arsitektur TI dirancang untuk memenuhi kebutuhan bisnis Bank, oleh karena itu Bank harus terlebih dahulu memiliki gambaran yang utuh mengenai bisnis Bank secara keseluruhan.

1) Kebutuhan Bisnis Bank

Beberapa teknik yang dapat digunakan untuk menguraikan bisnis Bank dalam rangka memperoleh gambaran yang utuh, antara lain:

a) Pemetaan kapabilitas bisnis (*business capability mapping*), yaitu dengan mengidentifikasi, mengategorikan, dan menguraikan kapabilitas bisnis yang dibutuhkan agar unit atau fungsi bisnis memiliki kemampuan untuk memberikan nilai kepada pemangku kepentingan;

b) Pemetaan organisasi (*organization mapping*), yaitu dengan menyusun representasi struktur organisasi bisnis (termasuk pihak ketiga), yang menggambarkan unit bisnis beserta unit/fungsi di bawahnya dan hubungan dalam organisasi (antarunit dan pemetaan terhadap kapabilitas bisnis, lokasi, serta atribut lain); dan

c) Pemodelan proses (*process modeling*), yaitu dengan menguraikan suatu fungsi bisnis untuk mengidentifikasi elemen proses antara lain aktivitas, peran, *input*, *output*, serta fungsi bisnis yang lebih detail atau spesifik.

2) Arsitektur Data

Arsitektur data mendefinisikan struktur dan interaksi dari jenis dan sumber data utama Bank, yang mencakup aset data logis, aset data fisik, serta sumber daya manajemen data (*data management resources*) yang diperlukan untuk mendukung kebutuhan bisnis.

Penyusunan arsitektur data akan menghasilkan, antara lain:

a) daftar jenis data yang dimiliki dan sarana penyimpanan data;

b) matriks korelasi jenis data dengan fungsi bisnis pada Bank; dan

c) matriks korelasi jenis data dengan aplikasi yang terkait.

3) Arsitektur Aplikasi

Arsitektur aplikasi mendefinisikan struktur dan interaksi aplikasi sebagai sekumpulan kapabilitas bisnis yang mendukung fungsi bisnis utama dan memproses data.

Penyusunan arsitektur aplikasi akan menghasilkan, antara lain:

a) daftar aplikasi yang dimiliki;

b) matriks korelasi aplikasi dengan fungsi bisnis pada Bank;

c) matriks korelasi aplikasi dengan unit kerja pada Bank; dan

d) matriks interaksi antar-aplikasi.

4) Arsitektur Teknologi

Arsitektur teknologi mendefinisikan struktur dan interaksi dari layanan teknologi serta komponen teknologi yang digunakan untuk mendukung aplikasi, data, dan kebutuhan bisnis Bank. Layanan teknologi merupakan layanan TI atau kapabilitas yang didukung oleh teknologi, seperti konektivitas jaringan dan layanan penyimpanan dan rekam cadang (*backup*). Komponen teknologi

merupakan aset TI yang mendukung layanan teknologi, antara lain jaringan, *middleware*, dan pangkalan data.
Penyusunan arsitektur teknologi akan menghasilkan, antara lain:
a) daftar teknologi yang digunakan Bank, termasuk perangkat keras dan perangkat lunak;
b) matriks pemetaan aplikasi terhadap teknologi; dan
c) diagram jaringan dan komunikasi yang menggambarkan koneksi antar aset TI Bank.

Selanjutnya, Bank menetapkan rencana pengembangan TI sesuai dengan arsitektur data, arsitektur aplikasi, dan arsitektur teknologi. Hal ini meliputi:
1) menyusun peta jalan (*roadmap*), termasuk rencana implementasi dan migrasi;
2) menetapkan mekanisme penilaian kesuksesan; dan
3) melakukan estimasi kebutuhan sumber daya dan jangka waktu penyelesaian.

c. Tahap Implementasi

Pada tahap implementasi, Bank mengimplementasikan rencana pengembangan TI yang telah ditetapkan dan memastikan setiap tahapan selaras dengan arsitektur TI yang telah disusun.

d. Tahap Kontrol

Pada tahap kontrol, Bank melakukan evaluasi atas kesesuaian pengembangan TI dengan peta jalan arsitektur TI secara berkala. Selain itu, Bank juga perlu mengkaji relevansi arsitektur TI yang ada terhadap kondisi dan perkembangan bisnis Bank secara berkala, terutama dalam hal terdapat perubahan atas faktor pertimbangan sebagaimana dimaksud pada butir A.1.

B. Rencana Strategis TI

1. Penyusunan Rencana Strategis TI

Sebagaimana diatur dalam Pasal 12 POJK PTI Bank wajib memiliki RSTI. RSTI disusun untuk mendukung rencana korporasi Bank. RSTI disusun untuk penyelenggaraan TI dalam jangka panjang sesuai periode rencana korporasi Bank.
Contoh:
Bank “AS” memiliki rencana korporasi dengan periode 5 (lima) tahunan, yang dimulai tahun 2026 sampai dengan tahun 2030, maka RSTI yang disusun oleh Bank “AS” juga harus sesuai dengan periode tersebut yaitu RSTI tahun 2026 sampai dengan 2030.
RSTI dituangkan dalam dokumen yang menggambarkan visi dan misi TI Bank, strategi pendukung, serta prinsip-prinsip utama yang menjadi acuan dalam penggunaan TI. Proses penyusunan dilakukan oleh satuan kerja TI, satuan kerja pengguna TI, dan komite pengarah TI.

a. Dokumen RSTI memuat paling sedikit:
1) visi dan misi TI Bank, yang menggambarkan secara jelas kesesuaian dengan visi dan misi Bank;
2) target perkembangan usaha Bank;
3) identifikasi kemampuan sumber daya TI Bank saat ini;
4) perencanaan TI untuk mendukung pencapaian target perkembangan usaha Bank, termasuk dengan estimasi biaya yang diperlukan;

5) analisis kesenjangan (*gap analysis*) antara kemampuan sumber daya TI yang ada saat ini, dengan yang diperlukan untuk mendukung target perkembangan usaha Bank; dan
6) strategi TI untuk mencapai kemampuan sumber daya TI yang dibutuhkan, serta dijabarkan melalui peta jalan (*roadmap*).

b. Dalam penyusunan RSTI, Bank memperhatikan antara lain:
1) kesesuaian arah dengan rencana strategis Bank secara keseluruhan;
2) kesesuaian arah dengan strategi dan kegiatan masing-masing unit bisnis, kondisi pasar, struktur demografi, dan segmentasi nasabah;
3) pemahaman manajemen mengenai peran dari TI dalam mendukung pelaksanaan kegiatan usaha Bank yang ada sekarang dan yang direncanakan;
4) pemahaman manajemen mengenai hubungan antara sumber daya TI yang digunakan sekarang dan yang direncanakan dengan strategi dan rencana kerja dari satuan kerja pengguna TI;
5) analisis manfaat langsung dan tidak langsung yang akan diperoleh dibandingkan dengan biaya yang akan dikeluarkan untuk penggunaan teknologi;
6) kebutuhan akan investasi baru di bidang teknologi;
7) rencana kebutuhan SDM;
8) kesesuaian dengan ketentuan peraturan perundang-undangan; dan
9) perkembangan teknologi.

2. Perubahan Rencana Strategis TI

Dalam hal terdapat kondisi yang secara signifikan memengaruhi sasaran dan strategi TI Bank sebagaimana dimuat dalam RSTI yang sedang berjalan, Bank dapat melakukan perubahan RSTI. Kondisi yang secara signifikan tersebut antara lain:

a. terjadi perubahan rencana korporasi, seperti penggabungan, peleburan, pengambilalihan, dan konversi, atau perubahan model bisnis Bank menjadi Bank digital; dan
b. perubahan ketentuan peraturan perundang-undangan yang berpengaruh terhadap penyelenggaraan TI Bank, seperti terdapat larangan untuk menyelenggarakan suatu teknologi terbaru yang dapat membahayakan keamanan data nasabah.

Dalam melakukan perubahan RSTI, Bank tetap memperhatikan hal dalam penyusunan RSTI sebagaimana tercantum dalam butir B.1.

BAB IV
PENERAPAN MANAJEMEN RISIKO PENYELENGGARAAN TI BANK

A. Proses Manajemen Risiko TI

Untuk melaksanakan Pasal 15 POJK PTI, Bank menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI. Cakupan penerapan manajemen risiko secara efektif dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum atau Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah. Manajemen risiko berlaku untuk seluruh penyelenggaraan TI antara lain keamanan siber, pengelolaan data, penggunaan PPJTI, dan penggunaan TI secara umum.

Penerapan manajemen risiko dilakukan secara terintegrasi dalam setiap tahapan penyelenggaraan TI, antara lain proses perencanaan, pengembangan, operasional, pemeliharaan, penghentian, dan penghapusan sumber daya TI. Sumber daya TI mencakup antara lain perangkat keras, perangkat lunak, jaringan, sumber daya manusia, data, dan informasi.

Bank wajib memastikan kecukupan sistem informasi manajemen risiko dalam penyelenggaraan TI. Sistem informasi manajemen dimaksud harus dapat menghasilkan laporan yang lengkap dan akurat dalam rangka mendeteksi dan mengoreksi penyimpangan secara tepat waktu. Selain itu, Bank juga perlu memiliki mekanisme pelaporan yang dapat memberikan informasi sesuai kebutuhan.

Dalam menerapkan manajemen risiko TI, Bank melakukan proses sebagai berikut:

1. Identifikasi Risiko

Dalam melakukan identifikasi dan penilaian risiko TI, Direksi harus memastikan adanya *risk awareness* di seluruh lini Bank, yaitu:

a. *risk awareness* dari Direksi dan pejabat pada seluruh jenjang jabatan;
b. pemahaman yang jelas mengenai *risk appetite* dari Bank;
c. pemahaman terhadap ketentuan peraturan perundang-undangan dan standar yang berlaku terkait TI; dan
d. transparansi dan integrasi tanggung jawab mengenai risiko yang signifikan dari setiap aspek terkait penyelenggaraan TI.

Untuk dapat memastikan hal di atas, Bank dapat menjalankan program *risk awareness* bagi seluruh pegawai dan manajemen Bank atau menjalankan metode lain yang dapat meningkatkan kesadaran para pengguna TI akan risiko yang ada.

Identifikasi risiko TI juga dapat dilakukan melalui pengumpulan data atau dokumen atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko, baik dari kegiatan yang sedang maupun yang akan berjalan, antara lain:

a. aset TI yang kritikal, dalam rangka mengidentifikasi titik-titik akses dan penyimpangan terhadap informasi nasabah yang bersifat rahasia;
b. hasil kaji ulang rencana strategis Bank;
c. hasil uji tuntas (*due dilligence*) dan pemantauan terhadap kinerja PPJTI;
d. hasil kaji ulang atas laporan atau keluhan yang disampaikan oleh nasabah dan/atau pengguna TI kepada *call center* dan/atau *helpdesk*;

e. hasil penilaian sendiri (*self assessment*) yang dilakukan seluruh satuan kerja terhadap pengendalian yang dilakukan terkait TI;
f. temuan audit terkait penyelenggaraan TI; dan
g. evaluasi terhadap penggunaan teknologi baru dan perubahan model bisnis Bank.

2. Pengukuran Risiko

Bank perlu memperhatikan signifikansi dampak risiko yang telah diidentifikasi oleh Bank terhadap kondisi Bank dan frekuensi terjadinya risiko. Metode yang digunakan Bank dapat berupa metode kuantitatif maupun kualitatif tergantung kompleksitas usaha dan TI yang digunakan. Dalam metode kualitatif, besarnya dampak dan kemungkinan terjadinya risiko (*likelihood*) dapat dijelaskan secara naratif atau dengan pemberian peringkat.

Contoh metode kualitatif pengukuran yang sederhana berupa penggunaan *check list* atau *subjective risk rating* seperti *high*, *medium*, atau *low*.

Agar risiko yang telah diidentifikasi dan dinilai atau diukur dapat dipantau oleh manajemen maka Bank perlu memiliki dokumentasi risiko atau yang sering disebut sebagai *risk register*.

Contoh pembuatan *risk register* mencakup:

a. penetapan aset, proses, produk, atau kejadian yang mengandung risiko;
b. pengukuran atau pemeringkatan kemungkinan kejadian dan dampak (*inherent risk assessment*);
c. langkah penanganan terhadap risiko potensial (*potential risk treatment*), misalnya *Accept*, *Control*, *Avoid*, atau *Transfer* (ACAT).

   Dalam dokumentasi penanganan terhadap risiko potensial (*potential risk treatment*), Bank perlu memperhatikan antara lain *risk appetite*, fasilitas yang dapat digunakan sebagai *preventive control* atau *corrective control*, dan kesesuaian rencana mitigasi risiko dengan kondisi keuangan Bank.

   Dokumentasi penanganan terhadap risiko potensial perlu dikinikan secara berkala.

   Penanganan risiko potensial yang dapat diambil Bank sebagai berikut:

   1) *Accept*

      Bank memutuskan untuk menerima risiko apabila besarnya dampak dan tingkat kecenderungan masih dalam batas toleransi organisasi.

      Contoh:

      a) Penetapan kriteria penerimaan risiko terkait dengan evaluasi dan penanganan risiko misalnya nilai risiko akhir "*low*".
      b) Penetapan nilai risiko akhir "*medium*" atau "*high*", namun telah diputuskan untuk diterima oleh Bank dan dibuat suatu sistem prosedur untuk memantau risiko tersebut.

   2) *Control*

      Organisasi memutuskan mengurangi dampak maupun kemungkinan terjadinya risiko.

      Contoh: pemasangan *firewall* pada *Personal Computer* (PC) untuk mencegah akses yang tidak terotorisasi.

3) *Avoid*
Organisasi memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan *output* yang sama untuk menghindari terjadinya risiko.
Contoh:
Pengguna tidak diberikan hak *privilege* sebagai administrator untuk menghindari risiko TI berupa *malicious code* pada PC akibat dari perubahan konfigurasi dan pemasangan perangkat lunak pada PC yang dilakukan oleh pengguna.
4) *Transfer*
Organisasi memutuskan untuk mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.
Contoh:
Mengasuransikan fasilitas ruangan atau gedung yang mengandung risiko terjadi kebakaran; dan

d. pengukuran atau pemeringkatan kemungkinan kejadian dan dampak setelah ACAT (*residual risk assesment*).

3. Pemantauan Risiko

Bank melakukan pemantauan risiko TI dengan mengevaluasi kesesuaian, kecukupan, dan efektivitas kinerja penyelenggaraan TI.

a. Hal yang dapat menjadi cakupan dalam evaluasi antara lain:
1) hasil audit dan kajian terkait;
2) umpan balik (*feedback*) yang diterima;
3) kebijakan, standar, dan prosedur serta penerapannya;
4) status dari tindakan preventif maupun korektif terkait risiko yang dihadapi Bank;
5) kelemahan dan ancaman baik yang telah ada maupun yang masih berupa potensi;
6) hasil pengukuran atas efektivitas penyelenggaraan TI;
7) tindak lanjut atas hasil evaluasi sebelumnya;
8) perubahan kondisi yang mempengaruhi penyelenggaraan TI; dan
9) rekomendasi untuk perbaikan atau penyempurnaan.

b. Tindak lanjut atas hasil evaluasi dapat dituangkan dalam bentuk keputusan maupun tindakan untuk meningkatkan efektivitas penyelenggaraan TI, antara lain:
1) penginian profil risiko, pengukuran risiko, dan rencana penanganan risiko;
2) penyempurnaan kebijakan, standar, dan prosedur di bidang TI;
3) pemenuhan kebutuhan SDM;
4) penetapan dan pelaksanaan tindakan preventif dan korektif berdasarkan asesmen atas ketidaksesuaian yang ada maupun yang masih bersifat potensi, dengan mempertimbangkan skala prioritas; dan
5) pemantauan dan evaluasi atas pelaksanaan tindakan preventif dan korektif.

c. Hasil evaluasi dan tindak lanjut sebagaimana dimaksud dalam huruf b harus didokumentasikan secara memadai.

4. Pengendalian Risiko

Bank harus menerapkan pengendalian risiko yang memadai sebagai bagian dari strategi mitigasi risiko TI secara keseluruhan dengan

memperhatikan paling sedikit:

a. hasil penilaian risiko;
b. kriteria penanganan risiko dan rekomendasi bentuk penanganan risiko;
c. ketentuan peraturan perundang-undangan dan persyaratan dalam perjanjian;
d. praktik pengendalian antara lain:
    1) penerapan kebijakan, standar, dan prosedur, serta struktur organisasi termasuk alur kerjanya;
    2) pengendalian intern yang efektif yang dapat memitigasi risiko dalam proses TI. Cakupan dan kualitas pengendalian intern merupakan kunci utama dalam proses manajemen risiko sehingga Bank harus mengidentifikasi persyaratan spesifik pengendalian intern yang diperlukan dalam setiap kebijakan dan prosedur yang diterapkan;
    3) penetapan kebijakan, standar, dan prosedur sistem pengelolaan pengamanan informasi yang diperlukan Bank untuk melakukan pengamanan aset terkait penyelenggaraan TI termasuk data atau informasi;
    4) evaluasi hasil kaji ulang dan pengujian atas Rencana Pemulihan Bencana (*Disaster Recovery Plan*/DRP);
    5) penetapan kebijakan dan prosedur mengenai penggunaan PPJTI. Direksi harus memiliki pemahaman secara menyeluruh atas risiko yang berhubungan dengan penggunaan jasa PPJTI untuk operasional TI;
    6) evaluasi terhadap pengamanan informasi yang dilakukan oleh PPJTI terhadap kerahasiaan, integritas data, dan ketersediaan informasi;
    7) pemakaian asuransi sebagai upaya untuk melengkapi mitigasi potensi kerugian dalam penyelenggaraan TI. Risiko yang perlu diasuransikan merupakan *residual risk*. Bank harus melakukan kaji ulang secara berkala atas kebutuhan, cakupan, dan nilai asuransi yang ditutup; dan
    8) melakukan pengawasan dan pemantauan terhadap PPJTI, mengingat operasional TI yang dilaksanakan oleh PPJTI tetap merupakan tanggung jawab dari Bank.

B. Pengamanan Informasi Dalam Penyelenggaraan TI Bank

Informasi merupakan aset yang sangat penting bagi Bank, antara lain informasi yang terkait dengan nasabah, keuangan Bank, dan laporan yang disusun oleh Bank. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan, atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun nonfinansial bagi Bank. Dampak dimaksud tidak hanya terbatas pada Bank, namun juga kepada nasabah.

Mengingat pentingnya informasi maka informasi harus dilindungi atau diamankan oleh seluruh personel Bank. Pengamanan informasi tidak hanya mencakup pengamanan terhadap semua aspek dan komponen TI terkait seperti perangkat lunak, perangkat keras, jaringan, peralatan pendukung (seperti sumber daya listrik dan sistem pendingin) serta SDM (seperti kualifikasi dan keterampilan), namun juga pengamanan informasi dalam bentuk yang lebih luas.

1. Pengamanan Informasi

Pengamanan informasi yang dilaksanakan secara efektif dan efisien, memperhatikan paling sedikit:

a. pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dengan memperhatikan kepatuhan terhadap ketentuan;
b. pengamanan informasi yang dilakukan terhadap aspek teknologi, SDM, proses, fisik, dan lingkungan dalam penyelenggaraan TI; dan
c. pengamanan informasi yang diterapkan berdasarkan hasil penilaian terhadap risiko (*risk assessment*) pada informasi yang dimiliki, dikelola, dan diproses oleh Bank.

Bank juga menerapkan pengamanan informasi secara komprehensif dan berkesinambungan yaitu dengan menetapkan kebijakan, standar, dan prosedur terkait pengamanan informasi, mengimplementasikan pengendalian pengamanan informasi, memantau dan mengevaluasi kinerja dan keefektifan kebijakan pengamanan informasi, serta melakukan penyempurnaan.

Di samping itu, Bank perlu mempertimbangkan implementasi standar dan/atau praktik terbaik (*best practices*) secara nasional maupun internasional di bidang pengamanan informasi, dengan memperhatikan tujuan, kebijakan usaha, ukuran, dan kompleksitas usaha Bank yang meliputi keragaman dalam jenis transaksi, produk, jaringan kantor, serta teknologi pendukung yang digunakan.

a. Kebijakan Pengamanan Informasi

Bank harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus sesuai dengan *risk appetite* Bank dan dikomunikasikan secara berkala kepada seluruh personel Bank dan pihak eksternal yang terkait. Di samping itu, perlu dilakukan evaluasi kebijakan secara berkala dan apabila terdapat perubahan penting.

Kebijakan tentang pengamanan informasi mencakup paling sedikit:

1) tujuan pengamanan informasi yang memuat paling sedikit pengelolaan aset, SDM, pengamanan fisik, pengamanan *logic* (*logical security*), pengamanan operasional TI, penanganan insiden pengamanan informasi, dan pengamanan informasi dalam pengembangan sistem;
2) komitmen Bank terhadap pengamanan informasi sejalan dengan strategi dan tujuan bisnis;
3) kerangka acuan dalam menetapkan pengendalian melalui pelaksanaan manajemen risiko Bank;
4) kepatuhan terhadap ketentuan internal dan ketentuan peraturan perundang-undangan;
5) pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi (*security awareness program*);
6) tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi;
7) sanksi atas pelanggaran kebijakan pengamanan informasi; dan
8) dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

b. Standar Pengamanan Informasi

Bank harus menetapkan standar pengamanan informasi sesuai dengan kebijakan pengamanan informasi antara lain dengan mengacu pada ketentuan peraturan perundang-undangan dan standar dan/atau praktik terbaik (*best practices*).

Standar tentang pengamanan informasi merupakan dasar untuk melaksanakan dan menilai kepatuhan pelaksanaan ketentuan terkait pengamanan informasi serta acuan untuk menyusun prosedur pengamanan informasi.

Contoh standar pengamanan informasi:

1) standar *password*;
2) standar enkripsi;
3) standar pengamanan server;
4) standar pengamanan perangkat jaringan;
5) standar pengamanan *end-point* atau komputer;
6) standar *logging*; dan
7) standar pengamanan aplikasi.

c. Prosedur Pengamanan Informasi

Bank harus memiliki prosedur pengamanan informasi terdiri atas:

1) Prosedur Pengelolaan Aset TI

Prosedur pengelolaan aset TI memuat paling sedikit:

a) aset TI dapat berupa data (*hardcopy* atau *softcopy*), perangkat lunak, perangkat keras, jaringan, serta perangkat pendukung, seperti sumber daya listrik dan sistem pendingin, serta SDM termasuk kualifikasi dan keterampilan;
b) aset TI diidentifikasi, ditentukan pemilik atau penanggungjawabnya, dan dicatat agar dapat dilindungi secara tepat;
c) pengaturan penggunaan informasi dan aset TI, seperti pengaturan penggunaan surat elektronik, internet, *mobile devices*, dan *teleworking*, harus diidentifikasi, didokumentasikan, dan diimplementasikan. Seluruh personel Bank dan pihak ketiga harus mematuhi pengaturan tersebut; dan
d) informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya. Klasifikasi dapat dibuat berdasarkan nilai, tingkat kerahasiaan, hukum atau ketentuan, dan tingkat kepentingan bagi Bank.

   Contoh dari klasifikasi tersebut:

   (1) informasi “rahasia” (misalnya data simpanan nasabah dan data pribadi nasabah), “internal” (misalnya peraturan tentang gaji pegawai Bank); dan
   (2) informasi “publik” (misalnya informasi tentang produk perbankan yang ditawarkan kepada masyarakat).

2) Prosedur Pengelolaan SDM

Prosedur pengelolaan SDM memuat paling sedikit:

a) Bank harus menerapkan pengendalian yang memadai sebelum mempekerjakan pegawai TI (tetap, kontrak, atau honorer), konsultan, termasuk pegawai

PPJTI pada posisi yang memiliki kerentanan atau dampak yang besar terhadap pengamanan informasi. Sebagai contoh yaitu melakukan *background check* catatan kriminal atau kejahatan lain seperti pencurian data saat melakukan rekrutmen untuk posisi *network administrator* atau *system administrator*;

b) SDM (pegawai Bank, konsultan, pegawai honorer, dan pegawai PPJTI) yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi;

c) peran dan tanggung jawab SDM (pegawai Bank, konsultan, pegawai honorer, dan pegawai PPJTI) yang memiliki akses terhadap informasi harus didefinisikan dan berdasarkan pada tingkat kebutuhan atas akses informasi serta didokumentasikan sesuai dengan kebijakan pengamanan informasi;

d) dalam perjanjian kerja dengan pegawai Bank (pegawai tetap dan pegawai tidak tetap) harus tercantum ketentuan-ketentuan mengenai pengamanan informasi yang sesuai dengan kebijakan pengamanan informasi Bank. Sebagai contoh, perlu adanya klausul yang menyatakan bahwa pegawai Bank (pegawai tetap dan pegawai tidak tetap) harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi;

e) dalam hal Bank bekerja sama dengan PPJTI (termasuk konsultan), perjanjian kerja sama antara Bank dengan PPJTI harus mencantumkan ketentuan mengenai pengamanan informasi, seperti klausul kerahasiaan informasi (*non-disclosure agreement*). Selain itu, semua pegawai yang ditugaskan PPJTI di Bank harus menandatangani suatu perjanjian menjaga kerahasiaan informasi dalam hal yang bersangkutan memiliki akses data Bank;

f) pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai Bank, konsultan, pegawai honorer, dan pegawai PPJTI. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab pegawai serta PPJTI;

g) Bank harus menetapkan sanksi atas pelanggaran yang dilakukan oleh SDM terhadap kebijakan pengamanan informasi; dan

h) Bank harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan pengubahan atau penutupan hak akses pegawai Bank, konsultan, pegawai honorer, dan pegawai PPJTI yang disebabkan karena perubahan tugas atau selesainya masa kerja atau perjanjian.

3) Prosedur Pengamanan Fisik dan Lingkungan

Prosedur pengamanan fisik dan lingkungan memuat paling sedikit:

a) fasilitas pemrosesan informasi yang penting (misalnya *mainframe*, server, komputer, dan

perangkat jaringan aktif) harus diberikan pengamanan secara fisik dan lingkungan yang memadai untuk mencegah akses oleh pihak tidak berwenang, kerusakan, dan gangguan lain;

b) pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk (misalnya penggunaan *access control card*, *Personal Identification Number* (PIN), dan *biometrics*), kelengkapan alat pengamanan di dalam ruangan, misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, dan kamera CCTV, serta pemeliharaan kebersihan ruangan dan peralatan, seperti dari debu, rokok, makanan, minuman, dan barang mudah terbakar;

c) fasilitas pendukung seperti sistem pendingin, sumber daya listrik, dan *fire alarm* harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;

d) aset milik PPJTI seperti server dan *switching tools* harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai, misalnya dengan menerapkan pengamanan yang cukup, *dual control* atau menempatkan secara terpisah dari aset Bank; dan

e) pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan.

4) Prosedur Pengendalian Akses

Prosedur pengendalian akses memuat paling sedikit:

a) pengendalian akses fisik dan *logic*;

b) Bank harus menerapkan metode identifikasi dan autentikasi (*authentication*) sesuai analisis risiko. Metode autentikasi yang digunakan dapat berupa satu atau kombinasi dari:
   (1) "*what you know*" (antara lain PIN dan *password*);
   (2) "*what you have*" (antara lain telepon seluler, kartu magnetis dengan *chip*, dan *token*); dan
   (3) "*something you are*" (antara lain *biometric* seperti retina dan sidik jari);

c) Bank harus memiliki prosedur formal tertulis dan telah disetujui oleh manajemen tentang pengadministrasian pengguna yang meliputi pendaftaran, perubahan dan penghapusan pengguna, baik untuk pengguna internal maupun eksternal Bank, misalnya vendor atau PPJTI;

d) pemberian akses mengacu kepada prinsip berdasarkan kebutuhan bisnis dan dengan akses yang seminimal mungkin;

e) Bank harus menetapkan prosedur pengendalian melalui pemberian *password* atau PIN awal (*initial password* atau PIN) kepada pengguna dengan memperhatikan antara lain:
   (1) *password* atau PIN awal harus diganti saat *login* pertama kali;

(2) *password* atau PIN diberikan secara aman, untuk memastikan misalnya melalui kertas karbon berlapis dua sehingga hanya diketahui oleh pihak yang berhak;
(3) *password* atau PIN awal bersifat acak khusus (*unique*) untuk setiap *user* dan tidak mudah ditebak;
(4) pemilik akun *user-id* terutama dari pegawai Bank, pegawai honorer, dan pegawai PPJTI harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan akun *user-id* dan *password* atau PIN saat menerima akun *user-id* dan *password* atau PIN awal; dan
(5) *password* atau PIN standar (*default password* atau PIN) yang dimiliki oleh sistem operasi, sistem aplikasi, *database management system*, serta perangkat jaringan dan keamanan harus diganti oleh Bank sebelum diimplementasikan dan mengganti akun *user-id* standar dari sistem (*default user-id*);

f) Bank harus mewajibkan pengguna untuk:
(1) menjaga kerahasiaan *password* atau PIN;
(2) menghindari penulisan *password* atau PIN di kertas dan tempat lain tanpa pengamanan yang memadai;
(3) memilih *password* atau PIN yang berkualitas yaitu:
(a) panjang *password* atau PIN yang memadai sehingga tidak mudah ditebak;
(b) mudah diingat dan terdiri dari paling sedikit kombinasi 2 (dua) tipe karakter (huruf, angka, atau karakter khusus);
(c) tidak didasarkan atas data pribadi pengguna seperti nama, nomor telepon atau tanggal lahir; dan
(d) tidak menggunakan kata yang umum dan mudah ditebak oleh perangkat lunak (untuk menghindari *brute force attack*);
(4) mengubah *password* atau PIN secara berkala; dan
(5) menghindari penggunaan *password* atau PIN yang sama secara berulang;

g) Bank harus menonaktifkan hak akses bila *user-id* tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan *password* atau PIN (*failed login attempt*), dan menonaktifkan pengguna setelah mencapai jumlah maksimal kegagalan *password* atau PIN;

h) Bank harus melakukan kaji ulang berkala oleh satuan kerja yang tidak terlibat dalam operasional pengendalian akses, terhadap hak akses pengguna untuk memastikan bahwa hak akses sesuai dengan wewenang yang diberikan;

i) sistem operasi, sistem aplikasi, pangkalan data (*database*), *utility*, dan perangkat lain yang dimiliki

oleh Bank dapat membantu pelaksanaan pengamanan *password* atau PIN, sebagai contoh:

(1) memaksa pengguna untuk mengubah *password* atau PINnya setelah jangka waktu tertentu dan menolak bila pengguna memasukkan *password* atau PIN yang sama dengan yang digunakan sebelumnya saat mengganti *password* atau PIN;
(2) menyimpan *password* atau PIN secara aman (terenkripsi);
(3) memutuskan hubungan atau akses pengguna jika tidak terdapat respons selama jangka waktu tertentu (*session time-out*); dan
(4) menonaktifkan atau menghapus hak akses pengguna jika pengguna tidak melakukan *log-on* melebihi jangka waktu tertentu (*expiration interval*), misalnya karena cuti, rotasi, dan mutasi; dan

j) Bank yang menggunakan *file* atau *folder sharing* harus menetapkan pembatasan akses paling sedikit melalui penggunaan *password* atau PIN dan pengaturan pihak yang berwenang melakukan akses.

5) Prosedur Pengamanan dalam Pengembangan dan Operasional TI

Prosedur pengamanan dalam pengembangan dan operasional TI memuat paling sedikit:

a) Bank juga harus memelihara catatan dari versi perangkat lunak yang digunakan dan memantau secara rutin informasi tentang penginian (*enhancement*) produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan;
b) Bank harus membuat prosedur yang mencakup identifikasi *patch* yang ada, melakukan pengujian dan melakukan instalasi jika memang dibutuhkan;
c) Bank harus menetapkan jenis *log* (misalnya *administrator log*, *user log*, atau *system log*) serta data yang harus dimasukkan ke dalam *log*, jangka waktu penyimpanan dengan memperhatikan ketentuan yang berlaku, untuk membantu investigasi di masa mendatang dan pemantauan pengendalian akses;
d) Bank harus melakukan kaji ulang secara berkala atas jejak audit atau *log* berdasarkan hasil analisis risiko baik di tingkat jaringan, sistem operasi, pangkalan data (*database*), maupun aplikasi;
e) Jejak audit atau *log* harus dilindungi terhadap gangguan dan akses tidak sah;
f) Penunjuk waktu dari seluruh Sistem Elektronik Bank harus disinkronisasikan dengan sumber penunjuk waktu akurat yang disepakati;
g) Bank harus melakukan kaji ulang secara berkala atas layanan operasional TI yang dilakukan oleh PPJTI. Periode kaji ulang harus ditetapkan dalam perjanjian kerja sama antara Bank dan PPJTI;
h) Bank harus menerapkan pengendalian media fisik dalam transit, untuk melindungi media terhadap akses yang tidak sah, penyalahgunaan, atau

kerusakan selama transportasi di luar batas fisik Bank; dan

i) Bank melakukan *secure coding*/*programming* dalam pengembangan TI.

6) Prosedur Pemantauan Pengamanan Informasi

Bank harus melakukan pemantauan dalam rangka mendeteksi upaya yang mengancam pengamanan informasi dengan metode yang ditentukan berdasarkan risiko atau tingkat kritikalitas informasi atau aset TI Bank. Pemantauan perlu dilakukan secara *realtime* untuk memberikan *alert* ketika terjadi aktivitas yang tergolong mencurigakan, misalnya *brute force attack* terhadap *password* administrator atau upaya mengakses server pada *port* yang tidak wajar, atau dilakukan secara berkala, misalnya pada akhir hari, berdasarkan tingkat risiko.

7) Prosedur Penanganan Insiden dalam Pengamanan Informasi

Hal yang harus diperhatikan Bank dalam melakukan penanganan insiden TI dalam pengamanan informasi antara lain:

a) Bank harus mengidentifikasi jenis insiden dalam pengamanan informasi misalnya pengguna dapat mengakses suatu sistem yang tidak diperbolehkan atau kelemahan (*vulnerabilities*) lain yang diketahui pengguna.

b) Pegawai Bank, pegawai honorer, dan pegawai PPJTI melaporkan setiap kali mengetahui, menemukan, atau melihat indikasi atau potensi insiden dalam pengamanan informasi sesuai huruf a).

c) Bank perlu mempertimbangkan pembentukan tim khusus yang menangani insiden pengamanan misalnya Tim Respon Insiden dalam Pengamanan Informasi (TRIPI) sesuai dengan ukuran dan kompleksitas usaha Bank.

d) Bank harus menetapkan beberapa hal terkait pelaporan insiden dalam pengamanan informasi sebagai berikut:

(1) unit kerja atau personel yang harus dihubungi apabila pegawai Bank, pegawai honorer, maupun PPJTI mengetahui adanya insiden dalam pengamanan keamanan informasi (*Point of Contact*/PoC);

(2) mekanisme pelaporan yang dapat digunakan untuk melaporkan insiden dalam pengamanan informasi oleh personel yang mengetahui terjadinya insiden;

(3) mekanisme verifikasi oleh PoC untuk meyakini bahwa laporan insiden dalam pengamanan informasi yang disampaikan pelapor sesuai dengan keadaan pada sistem baik sebelum maupun setelah pelapor menyampaikan bukti terjadinya insiden dalam pengamanan informasi; dan

(4) mekanisme *assessment* oleh PoC untuk menentukan kesesuaian laporan dengan jenis insiden keamanan informasi yang disampaikan

oleh pelapor. Dalam hal PoC telah menentukan bahwa laporan tersebut tergolong insiden dalam pengamanan informasi maka PoC harus segera menyampaikan laporan tersebut kepada TRIPI.

e) Bank harus menetapkan beberapa hal terkait penanganan insiden dalam pengamanan informasi sebagai berikut:
   (1) personel yang menjadi anggota TRIPI termasuk tugas dan tanggung jawabnya;
   (2) panduan untuk melakukan *assessment* terhadap kebenaran laporan insiden termasuk klasifikasi insiden dalam pengamanan informasi yang disampaikan PoC;
   (3) panduan penanganan insiden dalam pengamanan informasi yang akan dilakukan oleh TRIPI;
   (4) metode verifikasi oleh TRIPI untuk meyakini bahwa laporan insiden dalam pengamanan informasi yang disampaikan oleh PoC benar termasuk dalam kejadian yang diklasifikasikan sebagai insiden dalam pengamanan informasi. Dalam hal insiden dalam pengamanan informasi yang dilaporkan tersebut benar merupakan insiden dalam pengamanan informasi maka TRIPI harus menindaklanjuti insiden dalam pengamanan informasi tersebut sesuai panduan penanganan insiden dalam pengamanan informasi yang sesuai;
   (5) panduan TRIPI dalam melakukan penanganan terhadap insiden dalam pengamanan informasi sesuai jenisnya, mencakup langkah-langkah antara lain:
      (a) dokumentasi semua informasi mengenai insiden dalam pengamanan informasi;
      (b) identifikasi sistem TI yang terkena dampak insiden dalam pengamanan informasi;
      (c) isolasi terhadap sistem TI yang teridentifikasi terkena dampak insiden dalam pengamanan informasi;
      (d) pengumpulan semua informasi yang tersimpan dalam sistem TI yang diidentifikasi terkena dampak insiden dalam pengamanan informasi. Dalam hal informasi tersebut akan dijadikan barang bukti digital (*digital evidence*) maka pengumpulan (*collection*) dan penyimpanan (*preservation*) informasi harus dilakukan dengan metode *digital forensically sound*;
      (e) implementasi solusi terhadap insiden dalam pengamanan informasi sesuai dengan jenisnya dengan terlebih dahulu mendapat persetujuan manajemen;
      (f) dalam hal TRIPI mengidentifikasi bahwa insiden dalam pengamanan informasi tidak dapat dikendalikan, harus dilakukan eskalasi kepada manajemen untuk

mengaktifkan prosedur penanganan krisis; dan

(g) penyusunan laporan lengkap atas aktivitas penanganan insiden dalam pengamanan informasi untuk disampaikan kepada manajemen baik saat masih dalam proses penanganan maupun setelah solusi diimplementasikan dan insiden dalam pengamanan informasi berstatus *closed*;

(6) penginian terhadap panduan penanganan insiden dalam pengamanan informasi menggunakan *lesson learned* dari aktivitas penanganan insiden dalam pengamanan informasi sebelumnya.

f) Bank harus memelihara dokumentasi lengkap atas suatu insiden dalam pengamanan informasi.

g) Bank secara berkala melakukan kaji ulang terhadap panduan penanganan insiden dalam pengamanan informasi untuk memastikan panduan tersebut relevan dengan kondisi sistem TI Bank terkini.

h) Bank dapat mempertimbangkan pemberian insentif kepada pegawai Bank, pegawai honorer, dan pegawai PPJTI yang melaporkan insiden atau *vulnerabilities* TI yang berisiko dieksploitasi dan mengancam pengamanan informasi, dalam rangka mendorong tercapainya pengamanan informasi yang kuat atau memadai.

2. Jaringan Komunikasi

Jaringan komunikasi mencakup perangkat keras, perangkat lunak, dan media transmisi yang digunakan untuk mentransmisikan informasi berupa data, suara, gambar, dan video.

Penyelenggaraan jaringan komunikasi sangat dipengaruhi oleh perubahan TI, baik sistem maupun infrastruktur, dan rentan terhadap gangguan dan penyalahgunaan.

Oleh karena itu, Bank perlu memastikan bahwa integritas jaringan dipelihara dengan cara menerapkan kebijakan, standar, dan prosedur pengelolaan jaringan dengan baik, memaksimalkan kinerja jaringan, mendesain jaringan yang tahan terhadap gangguan, dan mendefinisikan layanan jaringan secara jelas serta melakukan pengamanan yang diperlukan.

Bank harus memiliki kebijakan, standar, dan prosedur sebagai pedoman dalam menyediakan jaringan komunikasi untuk meyakini bahwa kelangsungan operasional dan keamanan jaringan komunikasi tetap terjaga. Kebijakan jaringan komunikasi merupakan arah dan tujuan pengelolaan jaringan komunikasi yang akan diselenggarakan Bank, misalnya terkait dengan penerapan enkripsi pada jaringan komunikasi.

Standar jaringan komunikasi merupakan sejumlah parameter yang ditetapkan oleh Bank untuk memenuhi kebijakan jaringan komunikasi, misalnya penggunaan *Secure Socket Layer* (SSL).

Prosedur jaringan komunikasi merupakan serangkaian langkah teknis yang akan dilakukan oleh Bank untuk memenuhi standar jaringan komunikasi.

Kebijakan, standar, dan prosedur yang perlu ditetapkan mencakup paling sedikit:

a. pengukuran kinerja dan perencanaan kapasitas jaringan (*performance and capacity planning*);
b. pengamanan jaringan komunikasi (*network access control*, termasuk *remote access*);
c. *change management* (*setting*, *configuration*, dan *testing*);
d. *network management*, *network logging*, dan *network monitoring*;
e. penggunaan internet, intranet, surat elektronik (*e-mail*), dan *wireless* (termasuk mekanisme penggunaan jaringan komunikasi);
f. prosedur penanganan masalah (*problem handling*);
g. fasilitas rekam cadang (*backup*) dan pemulihan (*recovery*); dan
h. perjanjian dan SLA yang sesuai dengan kebutuhan Bank dan dipantau secara berkala apabila jaringan komunikasi yang digunakan oleh Bank diselenggarakan oleh PPJTI.

3. Rencana Pemulihan Bencana

Kegiatan perbankan tidak dapat terhindar dari adanya gangguan atau kerusakan yang disebabkan oleh alam dan/atau manusia misalnya terjadinya gempa bumi, bom, kebakaran, banjir, *power failure*, kesalahan teknis, kelalaian manusia, demo buruh, dan kerusuhan. Gangguan atau kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi Bank, tetapi juga berdampak pada kegiatan operasional bisnis Bank terutama pelayanan kepada nasabah. Apabila tidak ditangani secara khusus, Bank akan menghadapi risiko seperti risiko operasional dan risiko reputasi yang berdampak pada menurunnya tingkat kepercayaan nasabah kepada Bank.

Untuk meminimalisasi risiko tersebut, Bank harus memiliki Rencana Pemulihan Bencana. Rencana Pemulihan Bencana menekankan pada aspek teknologi dengan fokus pada pemulihan data (*data recovery* atau *restoration plan*) dan berfungsinya sistem aplikasi dan infrastruktur TI yang kritikal.

a. Kebijakan, Standar, dan Prosedur terkait Rencana Pemulihan Bencana

Kebijakan, standar, dan prosedur terkait Rencana Pemulihan Bencana mencakup paling sedikit:

1) Kebijakan terkait Rencana Pemulihan Bencana

Bank harus memiliki kebijakan terkait Rencana Pemulihan Bencana yang mendukung efektivitas pelaksanaan Rencana Pemulihan Bencana yang diperlukan yang memuat paling sedikit:

a) Penyusunan Tim Kerja Rencana Pemulihan Bencana
Bank perlu membentuk suatu organisasi atau tim kerja untuk mengoordinasikan pelaksanaan Rencana Pemulihan Bencana, yang terdiri atas:
(1) koordinator; dan
(2) anggota tim yang bertanggung jawab antara lain terhadap:
(a) satuan kerja bisnis; dan
(b) satuan kerja TI yang antara lain membawahkan fungsi pengelolaan *offsite storage*, aplikasi, perangkat keras, perangkat lunak, *network*, *security*, *communication*, dan *data preparation and records*.

Adapun peran tim kerja penanggung jawab Rencana Pemulihan Bencana paling sedikit:

(a) bertanggung jawab penuh terhadap efektivitas pelaksanaan Rencana Pemulihan Bencana, termasuk memastikan bahwa program *awareness* atas Rencana Pemulihan Bencana diterapkan;
(b) memutuskan kondisi bencana dan pemulihannya;
(c) menentukan skenario pemulihan yang akan digunakan apabila terjadi gangguan atau bencana berdasarkan skala prioritas atas aktivitas, fungsi, dan jasa yang dianggap kritis;
(d) melakukan kaji ulang atas laporan mengenai setiap tahapan dalam pengujian dan pelaksanaan Rencana Pemulihan Bencana; dan
(e) melaksanakan komunikasi kepada pihak internal dan eksternal Bank dalam hal terjadi gangguan operasional yang bersifat signifikan (*major*).

b) Prinsip-Prinsip Penyusunan Rencana Pemulihan Bencana

Dalam penyusunan kebijakan, strategi, dan prosedur yang akan diterapkan untuk menangani kondisi bencana, Bank harus memastikan diterapkannya prinsip sebagai berikut:

(1) Rencana Pemulihan Bencana disusun berdasarkan analisis dampak bisnis (*business impact analysis*) dan *risk assessment* yang memadai;
(2) Rencana Pemulihan Bencana bersifat fleksibel untuk dapat merespons berbagai skenario ancaman dan gangguan serta bencana yang sifatnya tidak terduga yang bersumber dari kondisi internal dan/atau eksternal;
(3) Rencana Pemulihan Bencana bersifat spesifik, terdapat kondisi tertentu dan tindakan yang dibutuhkan segera untuk mengatasi kondisi tersebut; dan
(4) Rencana Pemulihan Bencana dengan jelas menyatakan ketergantungan antar proses dan sistem dalam menjalankan proses bisnis kritikal.

c) Analisis Dampak Bisnis (*Business Impact Analysis*)

Efektivitas dari suatu Rencana Pemulihan Bencana bergantung pada kemampuan Bank untuk mengidentifikasi tingkat kepentingan (*criticality*) berbagai proses kerja atau aktivitas yang ada di Bank sebelum Rencana Pemulihan Bencana disusun atau dikaji ulang. Dengan demikian analisis dampak bisnis (*business impact analysis*) merupakan dasar dari penyusunan keseluruhan Rencana Pemulihan

Bencana. Hal yang harus dianalisis dalam analisis dampak bisnis (*business impact analysis*) meliputi:

(1) tingkat kepentingan (*criticality*) masing-masing proses bisnis dan ketergantungan antar proses bisnis serta skala prioritas yang diperlukan;
(2) ketergantungan antar proses dan sistem dalam menjalankan proses bisnis kritikal;
(3) tingkat ketergantungan terhadap pihak penyedia jasa baik TI maupun non-TI;
(4) jangka waktu Bank dapat beroperasi tanpa sistem atau fasilitas yang mengalami gangguan (*Maximum Tolerable Downtime*/MTD) dan/atau toleransi jangka waktu pemulihan sistem atau fasilitas tersebut hingga dapat berfungsi kembali (*Recovery Time Objective*/RTO), serta toleransi atas kehilangan data dan terhentinya proses bisnis (*Recovery Point Objective*/RPO);
(5) kebutuhan minimal jumlah personel, data, kelengkapan sistem, dan fasilitas yang diperlukan agar bisnis dapat beroperasi (*minimum resources requirement*);
(6) dampak potensial dari kejadian yang bersifat tidak spesifik dan tidak dapat dikontrol terhadap proses bisnis dan pelayanan kepada nasabah;
(7) dampak gangguan dan/atau bencana terhadap seluruh satuan kerja dan fungsi bisnis, bukan hanya terhadap *data processing*;
(8) jalur komunikasi yang dibutuhkan untuk berjalannya pemulihan; dan
(9) dampak hukum dan pemenuhan ketentuan yang terkait, seperti ketentuan peraturan perundang-undangan mengenai kerahasiaan data nasabah.

Dalam melakukan analisis dampak bisnis (*business impact analysis),* baik satuan kerja TI maupun masing-masing unit bisnis perlu memperhatikan bahwa Rencana Pemulihan Bencana yang akan disusun bukan hanya untuk *total disaster*, melainkan juga untuk berbagai situasi bencana dan gangguan mulai dari yang bersifat *minor*, *major* sampai dengan *catastrophic*.

Dampak yang harus diperhatikan bukan hanya yang dapat diukur dengan jelas (*tangible impact*) seperti penalti akibat keterlambatan pembayaran bunga atau biaya lembur pegawai, melainkan juga yang tidak dapat diukur secara jelas (*intangible impact*) seperti kesulitan nasabah memperoleh pelayanan.

d) *Risk Assessment*

Risk Assessment yang terdiri dari identifikasi dan pengukuran risiko merupakan tahap kedua yang harus dilalui dalam penyusunan Rencana Pemulihan Bencana. Proses ini diperlukan untuk dapat mengetahui tingkat kemungkinan terjadi gangguan pada kegiatan Bank yang penting (*critical*) serta

dampaknya bagi kelangsungan usaha Bank. *Risk assessment* mencakup paling sedikit:

(1) melakukan analisis atas dampak gangguan atau bencana terhadap Bank, nasabah, dan industri keuangan;
(2) melakukan analisis kesenjangan (*gap analysis*) dengan membandingkan kondisi saat ini dengan langkah atau skenario yang seharusnya diterapkan; dan
(3) membuat peringkat potensi gangguan bisnis berdasarkan tingkat kerusakan (*severity*) dan kemungkinan terjadinya (*likelihood*).

e) Penyusunan Rencana Pemulihan Bencana

Penyusunan Rencana Pemulihan Bencana dilakukan setelah proses analisis dampak bisnis (*business impact analysis*) dan *risk assessment*. Adapun tujuan dan sasaran dari penyusunan Rencana Pemulihan Bencana antara lain:

(1) mengamankan aset penting Bank;
(2) meminimalisasi risiko akibat bencana misalnya dengan membatasi kerugian finansial, risiko hukum, dan risiko reputasi;
(3) memastikan operasional Bank tetap berjalan;
(4) memastikan ketersediaan layanan yang berkesinambungan kepada nasabah; dan
(5) mempersiapkan alternatif lain agar fungsi bisnis yang kritikal tetap dapat berjalan untuk menjaga kelangsungan operasi Bank.

Rencana Pemulihan Bencana terdiri dari kebijakan, strategi, dan prosedur yang diperlukan untuk dapat memastikan kelangsungan proses bisnis pada saat terjadinya gangguan atau bencana. Rencana Pemulihan Bencana harus memuat beberapa alternatif strategi yang dapat diambil Bank untuk mengatasi masing-masing jenis dan ukuran gangguan atau bencana. Strategi pemulihan tersebut disesuaikan dengan hasil analisis dampak bisnis (*business impact analysis*), analisis risiko, sumber daya yang dimiliki, serta kapasitas dan tingkat teknologi Bank. Setiap strategi yang dipilih hendaknya disertai analisis atau alasan yang melatarberlakangi dan harus didukung dengan sistem dan prosedur yang sesuai.

2) Prosedur terkait Rencana Pemulihan Bencana

a) Jenis Prosedur Rencana Pemulihan Bencana

Adapun jenis prosedur dalam Rencana Pemulihan Bencana antara lain:

(1) prosedur tanggap darurat (*emergency response - immediate steps*) untuk mengendalikan krisis pada saat terjadi gangguan dan/atau bencana, membatasi dampak kerugian, serta menentukan perlu tidaknya mendeklarasikan keadaan gangguan dan/atau bencana;
(2) prosedur pemulihan sistem yang memungkinkan kegiatan operasional Bank dapat kembali ke kondisi normal; dan

(3) prosedur sinkronisasi data yang digunakan untuk memastikan kesamaan antara data mesin produksi dengan data yang ada di *backup site* serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem.

b) Komponen Prosedur Rencana Pemulihan Bencana

Setiap prosedur Rencana Pemulihan Bencana mencakup paling sedikit komponen sebagai berikut:

(1) personel

Rencana Pemulihan Bencana harus secara jelas mengemukakan komposisi, wewenang, dan tanggung jawab tim pelaksana pemulihan sistem dan memiliki alur komunikasi yang terintegrasi; dan

(2) teknologi

prosedur yang disusun harus memperhatikan komponen teknologi yang dimiliki Bank seperti perangkat keras, perangkat lunak, fasilitas komunikasi, sampai dengan peralatan pemrosesan kegiatan operasional di masing-masing fungsi bisnis.

Selain itu Bank juga perlu memperhatikan ketersediaan Pusat Pemulihan Bencana, dokumentasi sistem, dan rekam cadang (*backup*) data.

c) Pusat Pemulihan Bencana

Bank harus memastikan ketersediaan Pusat Pemulihan Bencana sebagai rekam cadang (*backup*) Pusat Data yang dapat dioperasikan apabila Pusat Data tidak dapat beroperasi akibat gangguan dan/atau bencana. Sesuai dengan alternatif strategi yang dipilih Bank, Pusat Pemulihan Bencana dapat dikelola sendiri maupun oleh PPJTI. Dalam penyelenggaraan Pusat Pemulihan Bencana, Bank harus memperhatikan paling sedikit:

(1) Pusat Pemulihan Bencana hendaknya ditempatkan dengan mempertimbangkan eksposur risiko yang berbeda dari masing-masing Pusat Data dan Pusat Pemulihan Bencana;

(2) kondisi rentannya lokasi Pusat Pemulihan Bencana yang dipilih dengan kemungkinan huru-hara dan kerusuhan;

(3) Pusat Pemulihan Bencana harus memiliki pasokan listrik dan sarana telekomunikasi yang dapat menjamin beroperasinya Pusat Pemulihan Bencana;

(4) sistem di Pusat Pemulihan Bencana harus kompatibel dengan sistem yang digunakan pada Pusat Data dan harus disesuaikan jika terjadi perubahan pada Pusat Data;

(5) Pusat Pemulihan Bencana merupakan *restricted area*; dan

(6) waktu tempuh untuk terjaminnya proses pemulihan pada Pusat Pemulihan Bencana.

d) Rekam Cadang (*Backup*) Dokumentasi, Sistem, dan Data

Bank harus meyakini ketersediaan rekam cadang (*backup*) yang efektif dari informasi bisnis yang penting, perangkat lunak, dan dokumentasi terkait sistem dan pengguna untuk setiap proses fungsi bisnis yang penting (*critical*). Hal yang harus diperhatikan dalam rekam cadang (*backup*) dokumentasi, sistem, dan data paling sedikit:

(1) rekam cadang (*backup*) dimaksud harus disimpan di lokasi lain dari Pusat Data (*off site*). Setiap perubahan dan modifikasi harus didokumentasikan dan salinannya juga harus diperbarui;

(2) media rekam cadang (*backup*) harus disimpan di lingkungan yang aman di lokasi *off site* dengan standar sistem pengamanan yang memadai;

(3) *full system backup* harus dilakukan secara berkala. Jika terjadi perubahan sistem yang mendasar maka *full system backup* harus dilakukan sesegera mungkin;

(4) seluruh media rekam cadang (*backup*) menggunakan standar penamaan (*labelling*) untuk dapat mengidentifikasi penggunaan, tanggal, dan jadwal retensi;

(5) media rekam cadang (*backup*) harus diuji secara berkala untuk meyakini agar dapat digunakan pada saat diperlukan (keadaan *emergency*);

(6) Bank harus memiliki prosedur untuk pemusnahan (*disposal*) media rekam cadang (*backup*); dan

(7) Bank perlu memiliki dokumentasi antara lain terkait objek *back up*, bagaimana metode *back up*, dan periode melakukan *back up*.

e) Fasilitas Komunikasi

Bank harus memastikan bahwa terdapat jalur komunikasi di wilayah operasional Bank yang dapat digunakan pada saat gangguan dan/atau bencana, baik di lingkungan internal maupun dengan pihak eksternal Bank. Hal ini termasuk alternatif jalur komunikasi dalam hal jalur komunikasi utama tidak dapat digunakan.

b. 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. 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.

Jika Bank menggunakan PPJTI dalam kegiatan operasionalnya maka pengujian yang dilakukan juga perlu melibatkan pihak eksternal tersebut.

1) Ruang Lingkup Pengujian Rencana Pemulihan Bencana

Bank harus secara jelas menentukan fungsi, sistem, dan proses yang akan diuji. Hal yang perlu diuji antara lain meliputi efektivitas dari:

a) prosedur penetapan kondisi gangguan dan/atau bencana;
b) prosedur pemulihan atas data penting (*critical*); dan
c) pengembalian kegiatan operasional Bank dan Pusat Data ke lokasi unit bisnis dan Pusat Data semula.

Pengujian yang dilakukan harus didokumentasikan secara tertib dan dievaluasi untuk meyakini efektivitas dan keberhasilan pengujian. Dalam hal pada saat pengujian terdapat kelemahan maka Rencana Pemulihan Bencana tersebut perlu disempurnakan.

2) Skenario Pengujian (*Test Plan*) Rencana Pemulihan Bencana

Bank harus memiliki skenario pengujian untuk setiap uji coba yang akan dilakukan dan skenario tersebut harus dikaji kecukupannya. Pelaksanaan skenario tersebut tidak boleh mengganggu kegiatan operasional Bank. Hasil uji coba diharapkan dapat mendeteksi adanya kelemahan dari prosedur yang ada dalam rangka perbaikan Rencana Pemulihan Bencana.

Dalam hal ini, Bank perlu memvalidasi asumsi yang digunakan dalam skenario pengujian, antara lain:

a) kritikalitas fungsi proses bisnis atau sistem yang diuji;
b) volume transaksi; dan
c) strategi Rencana Pemulihan Bencana yang dipilih Bank.

3) Analisis dan Laporan Hasil Pengujian Rencana Pemulihan Bencana

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

a) penilaian ketercapaian tujuan pengujian;
b) penilaian atas validitas pengujian pemrosesan data;
c) tindakan korektif untuk mengatasi permasalahan yang terjadi;
d) deskripsi mengenai kesenjangan antara Rencana Pemulihan Bencana dan hasil pengujian serta usulan perubahan Rencana Pemulihan Bencana; dan
e) 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. Pemeliharaan Rencana Pemulihan Bencana dan Audit Intern

1) Pemeliharaan Rencana Pemulihan Bencana

Bank harus memastikan bahwa Rencana Pemulihan Bencana dapat digunakan setiap saat antara lain dengan menyimpan salinan dokumen Rencana Pemulihan Bencana di lokasi alternatif (*alternate site*).

Bank perlu memastikan pemahaman semua pihak di Bank maupun di PPJTI atas pentingnya Rencana

Pemulihan Bencana dan berpartisipasi aktif dalam pelaksanaan Rencana Pemulihan Bencana.

Di samping itu, setiap satuan kerja secara berkala harus melakukan *self assessment* kesesuaian analisis dampak bisnis (*business impact analysis*) dengan perubahan yang terjadi dalam kegiatan operasional baik yang diselenggarakan sendiri maupun oleh PPJTI.

Bank harus melakukan penginian Rencana Pemulihan Bencana untuk meyakinkan kesesuaiannya dengan kondisi eksternal maupun internal. Dalam melakukan penginian, hal yang perlu diperhatikan antara lain perubahan yang ada dalam proses bisnis, sistem, perangkat lunak, perangkat keras, *operating system*, personel atau *key staff*, dan *service providers*. Perubahan tersebut harus dianalisis pengaruhnya terhadap Rencana Pemulihan Bencana yang ada pada saat ini dan menentukan perbaikan yang dibutuhkan untuk mengakomodasi perubahan tersebut dalam Rencana Pemulihan Bencana terbaru. Selanjutnya, Rencana Pemulihan Bencana hasil penginian tersebut harus didokumentasikan dan didistribusikan kepada satuan kerja TI.

2) Audit Intern

Auditor intern harus melakukan pemeriksaan terhadap:

a) kesesuaian Rencana Pemulihan Bencana dengan kebijakan manajemen risiko Bank;
b) Rencana Pemulihan Bencana mencakup kegiatan kritikal berdasarkan analisis dampak bisnis (*business impact analysis*) yang telah dilakukan oleh Bank;
c) kecukupan Rencana Pemulihan Bencana untuk mengendalikan dan memitigasi risiko yang telah ditetapkan dalam *risk assessment*;
d) kecukupan prosedur pengujian Rencana Pemulihan Bencana;
e) efektivitas pelaksanaan pengujian Rencana Pemulihan Bencana; dan
f) keterkinian Rencana Pemulihan Bencana sesuai perkembangan kegiatan operasional Bank dan hasil pengujian terakhir.

Auditor intern harus mengomunikasikan hasil pemeriksaan dan memberikan rekomendasi kepada Direksi. Direksi hendaknya melakukan kaji ulang atas laporan hasil audit tersebut dan merencanakan penyempurnaan atau perbaikan.

Frekuensi pelaksanaan audit dapat dilakukan sesuai dengan kompleksitas dan kebutuhan Bank.

BAB V
PENGGUNAAN PIHAK PENYEDIA JASA TI DALAM PENYELENGGARAAN TI BANK

A. Pendahuluan

Penggunaan PPJTI merupakan penggunaan jasa pihak lain yang menyediakan solusi TI seperti perangkat lunak, perangkat keras, dan/atau dukungan teknis dan konsultasi dalam penyelenggaraan TI Bank, dan dilakukan secara berkesinambungan dan/atau dalam periode tertentu, sehingga menyebabkan Bank memiliki ketergantungan terhadap jasa yang diberikan.

Penggunaan PPJTI dapat mempengaruhi risiko Bank antara lain karena adanya kegagalan PPJTI dalam menyediakan jasa atau ketidakmampuan untuk mematuhi ketentuan peraturan perundang-undangan. Oleh karena itu, untuk memitigasi dan melakukan pengendalian risiko dari penggunaan PPJTI, Bank harus memiliki kemampuan dalam melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh PPJTI.

Selain itu, Otoritas Jasa Keuangan memiliki kewenangan untuk mengawasi semua aktivitas penyelenggaraan TI yang dilakukan sendiri oleh Bank atau PPJTI. Sehingga, pemeriksaan dan pengawasan Bank tidak boleh terhambat dengan adanya pengalihan fungsi-fungsi operasional Bank kepada PPJTI.

B. Kebijakan dan Prosedur

Bank yang menggunakan PPJTI wajib memiliki kebijakan dan prosedur sesuai dengan Pasal 29 ayat (3) POJK PTI. Kebijakan dan prosedur dalam penggunaan PPJTI memuat paling sedikit:

1. Proses Identifikasi Kebutuhan Penggunaan PPJTI

Untuk dapat mengidentifikasi kebutuhan penggunaan PPJTI, Bank terlebih dahulu mendefinisikan kebutuhan bisnis terhadap penggunaan PPJTI antara lain:

a. identifikasi secara spesifik mengenai fungsi atau aktivitas yang akan diserahkan penyelenggaraannya kepada PPJTI;
b. proses penilaian risiko yang dapat timbul akibat penyerahan penyelenggaraan fungsi atau aktivitas tersebut; dan
c. penetapan dasar yang akan digunakan untuk mengidentifikasi pengukuran pengendalian yang memadai.

Hasil dari pendefinisian kebutuhan di atas harus memuat dokumen yang berisi gambaran secara rinci mengenai keinginan Bank terhadap jasa atau layanan yang akan dikerjakan oleh PPJTI, yang berisi dari beberapa komponen sebagai berikut:

a. cakupan dan karakteristik dari layanan dan teknologi yang digunakan serta dukungan kepada nasabah;
b. tingkat layanan meliputi ketersediaan dan kinerja, manajemen perubahan (*change management*), kualitas layanan, keamanan, dan kelangsungan usaha;
c. karakteristik minimal yang harus dipenuhi oleh PPJTI yang akan digunakan seperti pengalaman, arsitektur TI dan sistem, pengendalian proses, kondisi keuangan, dan referensi mengenai reputasi;
d. pemantauan dan pelaporan meliputi kriteria yang akan digunakan dalam pemantauan dan pelaporan baik untuk Bank maupun untuk pihak ketiga;
e. persyaratan yang harus dipenuhi baik dari sisi sistem, data maupun pelatihan personel saat transisi atau migrasi ke sistem yang disediakan PPJTI;

f. jangka waktu, penghentian, dan isi minimal dari perjanjian; dan
g. perlindungan perjanjian terhadap kewajiban seperti pembatasan kewajiban dan ganti rugi serta asuransi.

Proses identifikasi kebutuhan penggunaan PPJTI dilakukan paling sedikit dengan:

a. Meneliti Potensi Calon PPJTI
   Dalam meneliti potensi calon PPJTI, Bank melakukan antara lain:
   1) pemantauan terhadap potensi calon PPJTI yang dapat memberikan jasa TI sesuai dengan kebutuhan pencapaian tujuan bisnis dan strategi TI Bank, secara berkelanjutan; dan
   2) evaluasi dan komparasi kinerja PPJTI yang sedang digunakan oleh Bank dengan alternatif calon PPJTI lain, untuk mengidentifikasi peluang atau kebutuhan mendesak dalam rangka mempertimbangkan kembali perjanjian kerja sama dengan PPJTI yang sedang digunakan oleh Bank.
b. Menyusun Kriteria PPJTI yang Dibutuhkan
   Kriteria PPJTI yang dibutuhkan dapat disusun atau ditetapkan berdasarkan jenis, signifikansi, dan kekritisan jasa atau layanan TI yang diberikan oleh PPJTI. Penyusunan kriteria PPJTI bertujuan untuk membantu Bank dalam mencari dan memilih PPJTI yang sesuai dengan kebutuhan Bank.
   Setelah menetapkan kriteria PPJTI yang dibutuhkan, Bank mengidentifikasi, mendokumentasi dan mengategorisasi PPJTI sesuai dengan kriteria yang telah ditetapkan untuk dapat di kelola.

2. Proses Pemilihan PPJTI

Selain memperhatikan Pasal 30 ayat (2) POJK PTI, dalam proses pemilihan PPJTI Bank harus memastikan hal tersebut dilakukan sesuai dengan praktik yang adil dan tidak bertentangan dengan ketentuan yang berlaku. Bank juga harus memiliki standar pemilihan PPJTI sesuai dengan kompleksitas jasa TI yang dibutuhkan Bank (*best fit*).

Tahapan proses pemilihan PPJTI yang dapat menjadi acuan bagi Bank:

a. Permintaan Proposal dari PPJTI

Proses pemilihan PPJTI dimulai dengan permintaan proposal dari PPJTI. Proposal yang diajukan harus menjelaskan secara rinci kebutuhan Bank seperti cakupan dan jenis pekerjaan yang akan dilakukan, ekspektasi tingkat layanan, jangka waktu penyelesaian, rincian biaya layanan, pengukuran pekerjaan dan pengendaliannya, pengamanan, dan kelangsungan bisnis.

Bank harus dapat memastikan kebijakan PPJTI yang terkait dengan kepentingan audit penyelenggaraan TI Bank untuk akses auditor intern, ekstern, maupun Otoritas Jasa Keuangan. Dengan demikian, data dan informasi yang diperlukan dari penyelenggaraan TI tetap dapat diperoleh secara tepat waktu setiap kali dibutuhkan meskipun TI tidak diselenggarakan sendiri oleh Bank.

b. Uji Tuntas (*Due Diligence*) PPJTI

Uji tuntas (*due diligence*) perlu dilakukan untuk menilai reputasi, kemampuan teknis, kemampuan operasional, kondisi

keuangan, rencana pengembangan, dan kemampuan mengikuti inovasi TI di pasar, agar Bank mendapatkan keyakinan bahwa PPJTI mampu memenuhi kebutuhan Bank.
Pada saat uji tuntas (*due diligence*), Bank harus mempertimbangkan antara lain:

1) reputasi dan rekam jejak perusahaan PPJTI;
2) kualifikasi, latar belakang, dan reputasi pemilik perusahaan PPJTI;
3) perusahaan lain yang menggunakan jasa yang sama dari PPJTI sebagai referensi;
4) kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual;
5) teknologi dan arsitektur sistem;
6) lingkungan pengendalian intern, riwayat pengamanan informasi, dan cakupan audit;
7) kepatuhan terhadap hukum dan ketentuan peraturan perundang-undangan;
8) kepercayaan dan keberhasilan dalam berhubungan dengan subkontraktor;
9) jaminan pemeliharaan;
10) kemampuan untuk menyediakan pemulihan bencana dan keberlanjutan bisnis;
11) penerapan manajemen risiko;
12) laporan hasil audit TI yang dilakukan oleh pihak independen; dan
13) kondisi keuangan termasuk kaji ulang atas laporan keuangan yang telah diaudit.

Uji tuntas (*due diligence*) yang dilakukan Bank selama proses pemilihan harus didokumentasikan dengan baik dan dilakukan kembali secara berkala sebagai bagian dari proses pemantauan. Dalam melakukan uji tuntas (*due diligence*) secara berkala ini sebaiknya Bank memperhatikan perubahan atau perkembangan yang ada selama kurun waktu sejak uji tuntas (*due diligence*) terakhir dengan menggunakan informasi terkini.

c. Evaluasi Proposal PPJTI

Dalam tahap ini, Bank melakukan evaluasi paling sedikit terhadap kesesuaian aspek teknis dan aspek finansial, untuk setiap alternatif yang akan dipilih.

d. Penentuan PPJTI

Dalam menentukan PPJTI, Bank harus memperhatikan antara lain:

1) analisis biaya dan manfaat untuk setiap alternatif PPJTI yang akan dipilih, termasuk kewajarannya; dan
2) penerapan "hubungan kerja sama secara wajar (*arm's length principle*)" dengan PPJTI termasuk pihak terkait dengan Bank.

3. Hubungan Kerja Sama dengan PPJTI

Setelah memilih PPJTI, Bank membuat perjanjian kerja sama secara tertulis dengan PPJTI. Dalam menyusun perjanjian tertulis, Bank memperhatikan hal berikut:

a. isi perjanjian sesuai dengan standar perjanjian Bank. Bank harus memiliki standar isi perjanjian kerja sama dengan PPJTI yang memuat paling sedikit:
   1) cakupan pekerjaan atau jasa;
   2) biaya dan jangka waktu perjanjian kerja sama;

3) hak dan kewajiban Bank maupun PPJTI;
4) jaminan pengamanan dan kerahasiaan data;
5) jaminan tingkat pelayanan (*Service Level agreement*/SLA), berisi mengenai standar kinerja seperti tingkat pelayanan (*service level*) yang diperjanjikan dan target kinerja, termasuk dalam hal terjadi perubahan kepemilikan baik pada Bank maupun PPJTI;
6) laporan hasil pemantauan kinerja PPJTI yang terkait dengan SLA;
7) kesepakatan pembagian tanggung jawab atas risiko yang timbul di kemudian hari, antara lain:
   a) perubahan ruang lingkup pekerjaan dan/atau jangka waktu pelaksanaan;
   b) perubahan ruang lingkup bisnis dan organisasi PPJTI;
   c) perubahan regulasi; dan
   d) aspek hukum yang meliputi hak cipta, paten dan logo atau merek (*trade mark*);
8) persetujuan Bank secara tertulis dalam hal PPJTI melakukan pengalihan sebagian kegiatan (subkontrak) kepada subkontraktor, serta memastikan bahwa subkontraktor harus mempunyai standar penyelenggaraan TI yang memadai;
9) kesediaan PPJTI untuk memberikan akses kepada Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang untuk melakukan pemeriksaan terhadap kegiatan penyediaan jasa TI yang diberikan sesuai dengan ketentuan peraturan perundang-undangan;
10) PPJTI harus memberikan dokumen teknis kepada Bank terkait dengan jasa yang dikerjakan oleh PPJTI;
11) PPJTI harus melaporkan kepada Bank setiap kejadian kritis, yaitu kejadian yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank;
12) tanggung jawab PPJTI dalam menyediakan SDM yang memiliki kualifikasi dan kompetensi sesuai jasa yang disediakan agar operasional Bank tetap terjamin;
13) kesediaan PPJTI untuk melakukan alih pengetahuan kepada SDM Bank terkait dengan jasa TI yang disediakan;
14) perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal Otoritas Jasa Keuangan memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian;
15) sanksi dan penalti terhadap alasan-alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian; dan
16) kepatuhan pada hukum dan ketentuan peraturan perundang-undangan di Indonesia.

Selain standar isi perjanjian di atas, perjanjian kerja sama dengan PPJTI dapat juga memuat antara lain:
1) kepemilikan dan lisensi;
2) tersedianya sarana komunikasi yang terkoneksi dengan jaringan internet serta pengamanan terhadap akses dan transmisi data dari dan ke Pusat Data dan/atau Pusat Pemulihan Bencana;

3) pengaturan yang jelas mengenai rekam cadang (*back-up*) data, kebijakan saat keadaan yang mengancam kelangsungan operasional Bank (*contingency*), perlindungan terhadap data Bank (*record protection*) termasuk perangkat keras, perangkat lunak, dan perlengkapan (*equipment*), untuk menjamin kelangsungan penyelenggaraan TI;
4) untuk penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan pemrosesan transaksi berbasis TI, PPJTI menyampaikan kepada Bank, laporan keuangan terkini yang telah diaudit setiap tahun;
5) PPJTI menyampaikan kepada Bank hasil audit TI yang dilakukan auditor independen secara berkala;
6) komitmen bahwa PPJTI masih akan mendukung jasa yang diberikan kepada Bank selama periode tertentu setelah implementasi;
7) standar pengamanan sistem yang harus dipenuhi oleh PPJTI; dan
8) standar perjanjian penyimpanan dokumen (*escrow agreement*).

Muatan isi perjanjian di atas, diterapkan dengan mempertimbangkan skema, jenis layanan, dan/atau kompleksitas terkait penyediaan jasa TI yang digunakan oleh Bank, termasuk signifikansi dampak atas ketidaktersediaan jasa TI terhadap operasional Bank;

b. melalui proses pembahasan dengan satuan kerja hukum; dan
c. mempertimbangkan adanya klausul khusus untuk pemutusan perjanjian sebelum berakhirnya perjanjian apabila PPJTI wanprestasi. Dalam penggunaan klausul khusus, Bank harus memperhatikan hal berikut:
   1) Dalam perjanjian yang dibuat antara Bank dengan PPJTI harus dicantumkan klausul khusus mengenai kemungkinan mengubah, membuat perjanjian baru, atau mengambil alih kegiatan yang diselenggarakan oleh PPJTI atau menghentikan perjanjian sebelum berakhirnya perjanjian. Termasuk dalam hal ini atas permintaan Otoritas Jasa Keuangan apabila diperlukan dengan pertimbangan bahwa penyelenggaraan oleh PPJTI dapat mengganggu pelaksanaan tugas Otoritas Jasa Keuangan.
   2) Bank mampu mengukur risiko dan efisiensi dari penyelenggaraan TI yang diserahkan kepada PPJTI sehingga Bank dapat mengetahui secara dini bila terdapat kondisi-kondisi:
      a) hasil penilaian ulang materialitas menunjukkan bahwa kinerja PPJTI berpotensi tidak berjalan dengan efektif;
      b) memburuknya kinerja penyelenggaraan TI oleh PPJTI yang berpotensi menimbulkan dan/atau mengakibatkan dampak yang signifikan pada kegiatan usaha dan/atau operasional Bank;
      c) PPJTI menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan;
      d) terdapat pelanggaran terhadap ketentuan peraturan perundang-undangan mengenai rahasia Bank dan data pribadi nasabah;

e) terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan untuk pengawasan oleh Otoritas Jasa Keuangan; dan/atau
f) terdapat kondisi lain yang menyebabkan terganggunya atau terhentinya penyediaan jasa TI dari PPJTI kepada Bank.

3) Dalam hal Bank menemukan kondisi sebagaimana dimaksud pada angka 2) maka Bank harus melakukan tindakan paling sedikit:
a) melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi tersebut diketahui oleh Bank;
b) memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan PPJTI dalam hal diperlukan; dan
c) melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah Bank menghentikan penggunaan PPJTI sebelum berakhirnya jangka waktu perjanjian, dalam hal Bank memutuskan untuk menghentikan penggunaan PPJTI.

4) Untuk menjaga kelangsungan usaha Bank dalam hal penghentian penggunaan jasa TI dilakukan sebelum berakhirnya perjanjian Bank harus memiliki rencana tindak lanjut (*contingency plan*) yang teruji dan memadai dalam keadaan kahar (*force majeure*).

4. Proses Manajemen Risiko Penggunaan PPJTI

a. Identifikasi Risiko

Identifikasi risiko dalam penggunaan PPJTI paling sedikit memperhatikan hal sebagai berikut:

1) Penggunaan PPJTI lain dalam menyelenggarakan TI Bank dapat memberikan kontribusi terhadap beberapa jenis risiko, yaitu:
a) risiko operasional yaitu ketidakmampuan PPJTI dalam memenuhi perjanjian;
b) risiko hukum yaitu ketidakpastian hukum atas perselisihan dengan PPJTI, pihak ketiga, dan/atau tuntutan nasabah atas penyalahgunaan data nasabah oleh PPJTI;
c) risiko reputasi yaitu ketidakpuasan nasabah karena ketidakmampuan PPJTI memenuhi SLA;
d) risiko strategis yaitu ketidakcocokan TI yang digunakan Bank dengan tujuan dan rencana strategis Bank yang dibuat untuk mencapai tujuan tersebut;
e) risiko kepatuhan yaitu ketidakmampuan Bank memenuhi ketentuan peraturan perundang-undangan; dan
f) risiko negara (*country risk*) yaitu kondisi di negara asing yang dapat mempengaruhi kemampuan PPJTI dalam memenuhi standar pemberian jasa.

2) Dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko, Bank harus mempertimbangkan hal terkait dengan:
a) aktivitas dan fungsi yang diselenggarakan oleh PPJTI meliputi sensitivitas data yang diakses, dilindungi, atau dikendalikan oleh PPJTI, volume transaksi, dan

tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis Bank;

b) PPJTI seperti misalnya kondisi keuangan, kompetensi tenaga kerja, perputaran manajemen dan tenaga kerja, pengalaman PPJTI, dan profesionalitas; dan

c) teknologi yang digunakan meliputi keandalan (*reliability*), keamanan (*security*), ketersediaan (*availability*), dan ketepatan waktu (*timeliness*) serta kemampuan mengikuti perkembangan teknologi dan perubahan ketentuan peraturan perundang-undangan.

b. Pengukuran Risiko

Setelah risiko diidentifikasi, Bank harus mengukur risiko tersebut untuk mengetahui tingkat risiko yang dihadapi. Pengukuran risiko penggunaan PPJTI harus terintegrasi dengan pengukuran risiko terkait TI lain dengan menggunakan pendekatan pengukuran risiko yang sama. Hasil pengukuran risiko penggunaan PPJTI ini harus menghasilkan suatu tingkat risiko yang selanjutnya menjadi salah satu parameter untuk penilaian risiko TI Bank secara keseluruhan.

c. Mitigasi Risiko

Dari hasil pengukuran risiko, Bank mengetahui tingkat risiko yang dihadapi. Selanjutnya, Bank harus menetapkan strategi mitigasi risiko sesuai dengan tingkat risiko tersebut. Tindakan mitigasi risiko yang dilakukan Bank harus efektif untuk mengendalikan risiko.

1) tindakan mitigasi risiko yang dapat dilakukan Bank antara lain dengan menerapkan kontrol untuk mengurangi kemungkinan terjadinya risiko, antara lain:
   a) perjanjian PPJTI yang memadai;
   b) memantau kinerja penyedia jasa secara berkala; dan
   c) pemilihan PPJTI yang andal.
2) Tindakan mitigasi risiko lain yaitu mengurangi dampak kerugian apabila risiko yang telah diidentifikasi terjadi seperti asuransi dan Rencana Pemulihan Bencana.
3) Bank harus memastikan bahwa risiko ketergantungan pada PPJTI dapat dimitigasi sehingga Bank tetap mampu menjalankan bisnisnya apabila PPJTI mengalami wanprestasi, pemutusan hubungan, atau dalam proses likuidasi. Mitigasi risiko yang dapat dilakukan mencakup:
   a) memastikan bahwa PPJTI memiliki Rencana Pemulihan Bencana sesuai dengan jenis, cakupan dan kompleksitas aktivitas atau jasa yang diberikan;
   b) secara aktif mendapatkan jaminan kesiapan Rencana Pemulihan Bencana milik PPJTI seperti pengujian secara berkala atas Rencana Pemulihan Bencana;
   c) memiliki perjanjian penyimpanan program kode sumber (*escrow agreement*), jika Bank tidak memiliki kode sumber (*source code*) dari program aplikasi yang diselenggarakan oleh PPJTI; dan
   d) pemberian jaminan dari PPJTI kepada Bank bahwa kelangsungan aplikasi didukung oleh pejabat pengembang perangkat lunak dalam hal kode sumber (*source code*) tidak dimiliki oleh PPJTI.

4) Dalam rangka menjamin fungsi dan efektivitas Rencana Pemulihan Bencana, Bank harus menyusun dan melakukan pengujian Rencana Pemulihan Bencana secara berkala, lengkap, dan mencakup hal yang signifikan yang didasarkan atas jenis, cakupan, dan kompleksitas aktivitas atau kegiatan yang dilakukan oleh PPJTI. Di samping itu PPJTI harus melakukan pengujian Rencana Pemulihan Bencana pada PPJTI sendiri untuk sistem atau fasilitas TI maupun pemrosesan transaksi yang diselenggarakan tanpa melibatkan pihak Bank. Hasil pengujian Rencana Pemulihan Bencana oleh PPJTI tersebut digunakan Bank untuk mengkinikan Rencana Pemulihan Bencana yang dimiliki Bank.

d. Pengendalian Risiko Lain

Meskipun Bank maupun PPJTI sudah menggunakan sistem yang canggih, hal tersebut masih memungkinkan adanya penyimpangan misalnya kesalahan manusia, penerapan prosedur yang lemah, dan pencurian oleh pegawai. Bank harus memastikan adanya pengendalian pengamanan untuk memitigasi risiko dan mencakup:

1) PPJTI harus melakukan penelitian latar belakang para pegawainya;
2) memastikan kewajiban PPJTI melakukan pengendalian keamanan terhadap seluruh fasilitas TI yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian;
3) memastikan PPJTI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan Bank untuk masing-masing jenis data berdasarkan sensitivitas kerahasiaan data; dan
4) memastikan biaya yang dikeluarkan untuk masing-masing pengamanan sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko yang telah ditetapkan oleh Bank.

5. Tata Cara Penilaian Kinerja dan Kepatuhan PPJTI

Bank dalam melakukan penilaian kinerja dan kepatuhan PPJTI, memperhatikan antara lain:

a. pemantauan dan evaluasi keandalan PPJTI secara berkala terkait kinerja, reputasi PPJTI, dan kelangsungan penyediaan layanan;
b. penerapan pengendalian TI secara memadai oleh PPJTI, yang dibuktikan dengan hasil audit dan/atau penilaian yang dilakukan oleh pihak independen; dan
c. pemenuhan tingkat layanan (*Service Level Agreement*/SLA) sesuai dengan perjanjian tingkat layanan antara Bank dan PPJTI.

C. Penggunaan PPJTI di Luar Wilayah Indonesia

Bank yang merencanakan penggunaan PPJTI di luar wilayah Indonesia tidak boleh menghambat pengawasan atau pemeriksaan oleh Otoritas Jasa Keuangan. Sama halnya dengan penggunaan PPJTI domestik, penggunaan jasa TI pihak asing atau yang berlokasi di luar wilayah Indonesia harus memenuhi kebijakan dan prosedur yang sama, namun karena terkait dengan perbedaan yurisdiksi maka terdapat hal lain yang harus diperhatikan oleh Bank seperti ketersediaan akses bagi Otoritas Jasa Keuangan dalam melakukan pemeriksaan dalam hal diperlukan.

D. Penilaian Ulang Materialitas terhadap PPJTI

Bank perlu melakukan penilaian ulang terhadap PPJTI dalam hal terdapat perubahan organisasi PPJTI yang bersifat signifikan. Perubahan dimaksud antara lain perubahan kepemilikan atau perubahan kondisi keuangan PPJTI, yang dapat berdampak pada penyediaan jasa TI yang diberikan kepada Bank. Penilaian ulang dilakukan untuk menilai materialitas dari perubahan sifat, skala, dan kompleksitas risiko yang melekat pada penyediaan jasa TI.

Bank harus memiliki kebijakan, standar, dan prosedur atas penilaian ulang materialitas terhadap PPJTI yang memuat paling sedikit:

1. evaluasi keandalan terkait reputasi, kinerja, dan kelangsungan dari penyediaan layanan oleh PPJTI;
2. waktu penyelenggaraan penilaian ulang; dan
3. rencana tindak atas hasil penilaian ulang.

Penilaian ulang materialitas terhadap PPJTI dilakukan dengan memperhatikan antara lain:

1. penerapan prinsip hubungan kerja sama secara wajar;
2. potensi keberlangsungan penyediaan layanan oleh PPJTI; dan
3. penilaian kinerja dan kepatuhan PPJTI.

BAB VI
PENEMPATAN SISTEM ELEKTRONIK DAN PEMROSESAN TRANSAKSI BERBASIS TI

A. Penempatan Sistem Elektronik

Sesuai dengan Pasal 35 ayat (1) POJK PTI, dalam penyelenggaraan TI, Bank wajib untuk menempatkan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia.

Penempatan Sistem Elektronik dapat dilakukan di luar wilayah Indonesia, sepanjang Bank telah memperoleh izin dari Otoritas Jasa Keuangan dengan memenuhi ketentuan yang diatur dalam Pasal 35 ayat (3) dan Pasal 36 ayat (3) POJK PTI.

Dalam menempatkan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana di luar wilayah Indonesia, Bank harus tetap memastikan:

1. penerapan prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*);
2. jaminan kelangsungan usaha Bank; dan
3. tidak mengurangi efektivitas pengawasan Otoritas Jasa Keuangan.

Salah satu kriteria penempatan Sistem Elektronik di luar wilayah Indonesia yaitu Sistem Elektronik yang digunakan untuk manajemen intern. Yang dimaksud dengan Sistem Elektronik yang digunakan untuk manajemen intern yaitu sistem yang digunakan Bank untuk keperluan intern, yang tidak terkait secara langsung dengan pelayanan kepada nasabah dan/atau operasional Bank.

Sistem Elektronik yang digunakan untuk manajemen intern antara lain:

1. sistem kepegawaian;
2. sistem remunerasi;
3. sistem audit intern;
4. sistem pengolahan dokumen internal Bank;
5. aplikasi kolaborasi internal Bank; dan
6. aplikasi *knowledge management system*, termasuk yang memanfaatkan *artificial intelligence*.

B. Pemrosesan Transaksi Berbasis TI

Pasal 39 POJK PTI mengatur bahwa Bank wajib menyelenggarakan pemrosesan transaksi berbasis TI di wilayah Indonesia. Pemrosesan transaksi berbasis TI dapat dilakukan oleh PPJTI di wilayah Indonesia. Pemrosesan transaksi berbasis TI di luar wilayah Indonesia yang dilakukan oleh PPJTI dapat dilaksanakan sepanjang Bank memperoleh izin dari Otoritas Jasa Keuangan.

Pemrosesan transaksi berbasis TI yang dilakukan oleh PPJTI, baik yang berada di wilayah Indonesia atau di luar wilayah Indonesia, harus:

1. memenuhi prinsip kehati-hatian, antara lain:
    a. Bank menerapkan proses manajemen risiko dalam pelaksanaan pemrosesan transaksi berbasis TI oleh PPJTI;
    b. Bank memastikan penerapan prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) oleh PPJTI;
    c. Bank tetap bertanggung jawab atas pemrosesan transaksi dalam hal dilakukan oleh PPJTI; dan
    d. Bank menatausahakan dokumen yang digunakan dalam pemrosesan transaksi, termasuk yang dilakukan oleh PPJTI;
2. memperhatikan aspek pelindungan nasabah, termasuk penerapan prinsip pelindungan data pribadi; dan
3. dilaksanakan sesuai dengan ketentuan mengenai penggunaan PPJTI pada Bab V.

BAB VII
PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI DALAM PENYELENGGARAAN TI BANK

A. Pengelolaan Data

Dalam melaksanakan kewajiban sebagaimana dimaksud dalam Pasal 43 POJK PTI, Bank mengelola data secara efektif dalam pemrosesan data Bank untuk mendukung pencapaian tujuan bisnis Bank. Bentuk dari pemrosesan data yang dilakukan oleh Bank, antara lain perolehan, pendistribusian, pengolahan, pemeliharaan, penyimpanan, dan penghapusan data.

Dalam bisnis Bank, tujuan pengelolaan data yang utama yaitu untuk memungkinkan Bank mengelola data sebagai aset serta mengupayakan ketersediaan data yang andal dan akurat untuk agregasi risiko dan pelaporan termasuk akuntabilitas data dan kemampuan data untuk dapat ditelusuri. Pengelolaan data dilaksanakan oleh seluruh satuan kerja maupun individu pada Bank, tidak terbatas pada satuan kerja TI saja. Pengelolaan data harus melibatkan seluruh aspek SDM (*people*), proses (*process*), dan teknologi (*technology*) yang diperlukan untuk memastikan bahwa data yang diproses sesuai dengan tujuan yang dimaksudkan.

Dalam pengelolaan data, Bank harus memiliki kebijakan dan standar pengelolaan data yang mencakup paling sedikit aspek:

1. Kepemilikan dan Kepengurusan Data

Bank menetapkan pembagian tugas, wewenang, dan tanggung jawab dari setiap unit atau fungsi terkait pengelolaan data sesuai kompleksitas usaha Bank dengan memperhatikan kepemilikan data (*data ownership*) dan kepengurusan data (*data stewardship*).

2. Kualitas Data

Bank menetapkan standar kualitas data yang harus dipenuhi dalam pengelolaan data, antara lain:

a. akurasi;
b. kelengkapan;
c. konsistensi;
d. integritas;
e. kewajaran;
f. keterbaruan; dan
g. keunikan.

Bank melakukan pengembangan dan upaya menjaga dan/atau memperbaiki kualitas data, antara lain melalui:

a. penetapan standar, persyaratan, dan spesifikasi penerapan kontrol kualitas data;
b. identifikasi permasalahan terkait kualitas data;
c. upaya peningkatan kualitas data yang diidentifikasi; dan
d. evaluasi tingkat kualitas data.

3. Sistem Pengelolaan Data

Bank perlu membentuk sistem pengelolaan data yang komprehensif dan efektif, antara lain Bank:

a. memiliki arsitektur data sebagai bagian dari arsitektur TI;
b. menerapkan pelindungan data dan informasi yang mencakup:
   1) penetapan standar pengamanan data sesuai dengan klasifikasi data; dan
   2) implementasi kontrol dan prosedur pengamanan data dan informasi;

   Bank menetapkan klasifikasi data berdasarkan kritikalitas dan sensitivitas dari masing-masing jenis data. Bank menetapkan

metode untuk menjaga keamanan dan privasi data berdasarkan klasifikasi data yang telah ditetapkan. Metode dimaksud dapat berupa antara lain penerapan enkripsi, kontrol akses berbasis peran (*Role-Based Access Control*/RBAC), manajemen pengelolaan kunci (*key management*), otentikasi (*authentication*), dan metode lain;

c. Bank menetapkan standar interoperabilitas dan integrasi data untuk memungkinkan sistem yang berbeda dapat bertukar data secara efisien. Integrasi data merupakan penggabungan data ke dalam bentuk yang konsisten. Interoperabilitas data merupakan kemampuan beberapa sistem untuk berkomunikasi. Penerapan integrasi dan interoperabilitas data memastikan Bank dapat memperoleh data di mana pun, kapan pun, dan dalam bentuk apa pun sesuai kebutuhan;

d. menetapkan siklus pengelolaan untuk setiap fase data, mulai dari penciptaan (*creation*), penggunaan (*usage*), penyimpanan (*store*), pengarsipan (*archive*), retensi (*retention*), hingga pemusnahan (*disposal*);

e. Bank mengelola data *warehouse* dan/atau sistem aplikasi *business intelligence*; dan

f. Bank menetapkan kebijakan tentang pengelolaan metadata yang bertujuan untuk memastikan kualitas dan keamanan metadata. Metadata merupakan serangkaian data yang menjelaskan dan memberikan informasi mengenai data lain.

4. Sumber Daya Pendukung Pengelolaan Data

Sumber daya pendukung pengelolaan data antara lain berupa:

a. teknologi yang digunakan untuk mendukung sistem pengelolaan data; dan

b. SDM yang kompeten untuk melakukan pengelolaan data.

B. Pelindungan Data Pribadi

Dalam melakukan pemrosesan data pribadi, Bank wajib menerapkan prinsip pelindungan data pribadi sesuai dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi, sebagaimana diatur dalam Pasal 44 POJK PTI. Pemrosesan data pribadi yang dilakukan oleh Bank, harus memiliki dasar pemrosesan data pribadi sesuai dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi. Dalam hal pemrosesan data pribadi melibatkan pihak ketiga, Bank melakukan pengawasan pihak yang terlibat dalam pemrosesan data pribadi dimaksud.

Bank dapat menunjuk pejabat atau petugas yang bertanggung jawab untuk memastikan penerapan prinsip pelindungan data pribadi. Penunjukkan pejabat atau petugas tersebut, dilakukan dengan mempertimbangkan kompetensi yang dimiliki oleh pejabat atau petugas yang akan ditunjuk.

1. Persetujuan Pemrosesan Data Pribadi

Sebelum pemrosesan data pribadi nasabah dilaksanakan, Bank harus terlebih dahulu memperoleh persetujuan nasabah dan/atau calon nasabah secara eksplisit yang terdokumentasi dengan baik. Proses permintaan persetujuan nasabah dalam rangka pemrosesan data pribadi nasabah dan/atau calon nasabah dilakukan secara memadai, dengan memperhatikan antara lain:

a. permintaan persetujuan Bank tidak berupa persetujuan yang bersifat otomatis tanpa ada instruksi dari nasabah, seperti penggunaan kotak centang (*tick box*) yang telah dicentang sebelumnya atau jenis persetujuan otomatis lain;

b. permintaan persetujuan disusun dalam bahasa yang jelas, sederhana, dan mudah dimengerti;
c. Bank menginformasikan kepada nasabah tujuan permintaan data pribadi nasabah oleh Bank;
d. Bank memberikan opsi pilihan persetujuan untuk setiap tujuan dan jenis pemrosesan data pribadi yang berbeda;
e. Bank memberikan informasi legalitas dari pemrosesan data pribadi nasabah sesuai dengan ketentuan perundang-undangan;
f. Bank memberikan informasi hak nasabah untuk menarik persetujuan yang telah diberikan kepada Bank;
g. Bank memastikan bahwa nasabah memiliki hak untuk menolak pemberian persetujuan;
h. Bank tidak menjadikan pemberian persetujuan atas hal yang tidak terkait langsung dengan nasabah sebagai prasyarat pemberian layanan Bank; dan
i. Bank melakukan penghapusan data setelah masa retensi data pribadi (hanya untuk kepentingan *maintenance*/audit/rekam jejak) berakhir sesuai dengan peraturan perundang-undangan mengenai pelindungan data pribadi.

2. Analisis Dampak Pelindungan Data Pribadi

Pemrosesan data pribadi oleh Bank memiliki risiko antara lain eksploitasi data, kebocoran data, pelanggaran privasi, dan pencurian data. Oleh karena itu, Bank perlu mengidentifikasi kriteria data pribadi yang berisiko tinggi sesuai dengan kriteria yang diatur dalam peraturan perundang-undangan mengenai pelindungan data pribadi.

Dalam hal pada pemrosesan data pribadi terdapat kondisi tertentu yang berpotensi meningkatkan risiko bagi subjek data pribadi, Bank perlu melakukan penilaian dampak atas pelindungan data pribadi sesuai dengan Pasal 44 ayat (2) POJK PTI BU. Kondisi tertentu antara lain:

a. penggunaan teknologi baru;
b. pelacakan lokasi dan perilaku nasabah;
c. pemantauan atas lokasi fasilitas publik dalam skala besar; dan
d. pemrosesan data pribadi bersifat sensitif yang berkaitan dengan suku, agama, ras, dan antargolongan,

Penilaian dampak pelindungan data pribadi yang dilakukan oleh Bank memuat paling sedikit:

a. deskripsi mengenai kegiatan pemrosesan data pribadi dan tujuan pemrosesan data pribadi, termasuk kepentingan Bank atas pemrosesan data pribadi;
b. penilaian kebutuhan dan proporsionalitas antara tujuan dan kegiatan pemrosesan data pribadi;
c. penilaian risiko terhadap hak subjek data pribadi (yang dimaksud dengan subjek data pribadi yaitu orang perseorangan yang pada dirinya melekat data pribadi); dan
d. langkah Bank untuk melindungi subjek data pribadi dari risiko pemrosesan data pribadi.

3. Pertukaran Data Pribadi

a. Kebijakan, Standar dan Prosedur

Bank perlu memiliki kebijakan, standar, dan prosedur mengenai pertukaran data pribadi yang memadai, dengan memuat paling sedikit:

1) jenis data nasabah untuk pertukaran atau transfer data dan informasi;

2) persetujuan nasabah untuk pertukaran atau transfer data dan informasi;
3) mekanisme permintaan informasi oleh pihak eksternal dan pemberian informasi kepada pihak eksternal;
4) mekanisme transfer data;
5) media atau sarana yang diperkenankan untuk dipergunakan dalam pertukaran data dan informasi;
6) pengamanan jaringan komunikasi dan transmisi data dan informasi termasuk penggunaan enkripsi;
7) hak nasabah dalam transaksi yang melibatkan pertukaran atau transfer data dan informasi; dan
8) pembagian tanggung jawab pihak yang terlibat dalam pertukaran atau transfer data.

b. Perjanjian Kerja Sama

Dalam melakukan pertukaran data atau transfer data dengan pihak ketiga, Bank perlu memiliki perjanjian kerja sama yang memadai. Perjanjian kerja sama yang memadai antara Bank dan pihak ketiga memuat paling sedikit:

1) ruang lingkup dan durasi pemrosesan;
2) sifat dan tujuan pemrosesan;
3) jenis data pribadi dan kategori data nasabah;
4) kewajiban dan hak pengendali data pribadi, termasuk seluruh pihak yang terlibat dalam pemrosesan data;
5) aspek pengamanan data pribadi; dan
6) proses pertukaran data dalam keadaan darurat.

c. Klasifikasi Jenis Data

Bank perlu menetapkan klasifikasi jenis data pribadi serta kebijakan dan prosedur pertukaran data sesuai dengan klasifikasi jenis data yang telah ditetapkan. Bank harus menerapkan pengamanan atas data nasabah yang dipertukarkan sesuai dengan klasifikasi data. Penetapan klasifikasi jenis data yang dapat menjadi acuan bagi Bank antara lain:

1) data yang disediakan oleh nasabah/calon nasabah;
2) data transaksi;
3) data yang telah memiliki nilai tambah (*value-added*) dari data yang disediakan oleh nasabah/calon nasabah; dan
4) data agregat.

BAB VIII
PENYEDIAAN JASA TI OLEH BANK

A. Pendahuluan

Dalam menyelenggarakan TI, Bank memerlukan infrastruktur TI yang memadai. Penyediaan infrastruktur tersebut dapat dilakukan sendiri oleh Bank ataupun oleh PPJTI. Dalam hal Bank menyediakan infrastruktur TI secara mandiri, ada kemungkinan bahwa infrastruktur dimaksud belum terpakai secara penuh (*idle*) sehingga menjadi tidak efisien. Oleh karena itu dalam rangka meningkatkan efisiensi, Bank dapat menyediakan jasa TI. Selain itu, penyediaan jasa TI oleh Bank juga dapat dilakukan dalam rangka mendukung sinergi antarbank dan/ atau lembaga jasa keuangan.

Sebagaimana diatur dalam Pasal 48 POJK PTI, Bank hanya dapat menyediakan jasa TI kepada lembaga jasa keuangan lain:

1. yang diawasi oleh Otoritas Jasa Keuangan; dan/atau
2. di luar wilayah Indonesia yang diawasi otoritas pengawas dan pengatur lembaga jasa keuangan setempat.

Penyediaan jasa TI yang dapat diberikan Bank antara lain penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan aplikasi, serta jaringan komunikasi.

Penyediaan jasa TI berupa aplikasi kepada lembaga jasa keuangan selain bank dapat dilakukan sepanjang lembaga jasa keuangan pengguna jasa TI berada dalam satu grup atau kelompok dengan Bank dan penggunaan aplikasi ditujukan untuk mendukung kegiatan operasional yang umum. Yang dimaksud dengan "kegiatan operasional yang umum" yaitu kegiatan yang tidak spesifik terhadap jenis lembaga jasa keuangan. Contoh aplikasi yang ditujukan untuk mendukung kegiatan operasional yang umum antara lain sistem remunerasi dan sistem kepegawaian.

Keputusan penyediaan jasa TI pada dasarnya harus mempertimbangkan faktor efisiensi dan risiko. Oleh karena itu, penyediaan jasa TI harus memenuhi ketentuan Otoritas Jasa Keuangan dan harus:

1. mendapatkan persetujuan pejabat Bank yang berwenang;
2. memiliki perjanjian penyediaan jasa TI yang memungkinkan adanya klausul kondisi pemutusan perjanjian sesuai dengan jangka waktu perjanjian maupun sebelum perjanjian berakhir;
3. menetapkan peran dan tanggung jawab dari pihak-pihak yang terkait dengan penyediaan jasa TI; dan
4. mengevaluasi calon penerima jasa TI antara lain berdasarkan kondisi keuangan dan reputasi.

B. Kebijakan, Standar, dan Prosedur

1. Kebijakan dan Standar Penyediaan Jasa TI oleh Bank

Bank harus memiliki kebijakan standar penyediaan jasa TI oleh Bank yang mencakup paling sedikit:

a. standar isi perjanjian kerja dengan penerima jasa TI;
b. cakupan pekerjaan atau jasa;
c. jangka waktu perjanjian penyediaan jasa TI;
d. hak dan kewajiban Bank maupun penerima jasa TI;
e. jaminan pengamanan dan kerahasiaan data. Khusus untuk menjaga kerahasiaan data Bank sebagai pengguna aplikasi maka Bank sebagai penyedia jasa TI harus memisahkan paling sedikit pangkalan data (*database*) yang disesuaikan dengan arsitektur aplikasi Bank sebagai penyedia jasa TI;
f. jaminan tingkat pelayanan (*Service Level Agreement*/SLA), berisi mengenai standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service level*) dan target kinerja;

g. SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penerima jasa TI;
h. kesepakatan pembagian tanggung jawab atas risiko yang timbul di kemudian hari, antara lain:
   1) perubahan ruang lingkup pekerjaan dan/atau jangka waktu pelaksanaan;
   2) perubahan regulasi; serta
   3) aspek hukum yang meliputi hak cipta, paten, dan logo atau merek (*trade mark*);
i. pengaturan yang jelas mengenai perlindungan terhadap data Bank (*record protection*) termasuk infrastruktur pendukung berupa perangkat keras, perlengkapan (*equipment*), dan perangkat lunak, untuk menjamin kelangsungan penyelenggaraan TI;
j. kepemilikan dan lisensi (*license*) dalam hal penyediaan jasa TI berupa aplikasi;
k. perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal Otoritas Jasa Keuangan memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian;
l. sanksi dan penalti terhadap alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian;
m. kepatuhan pada ketentuan peraturan perundang-undangan di Indonesia; dan
n. standar pengamanan sistem yang harus dipenuhi.

2. Prosedur Penyediaan Jasa TI oleh Bank

Bank harus memiliki prosedur penyediaan jasa TI oleh Bank yaitu prosedur pendefinisian kebutuhan penerima jasa TI. Pendefinisian kebutuhan bisnis penerima jasa terhadap penyediaan jasa TI oleh Bank harus dilakukan sebelum Bank memutuskan menyediakan jasa TI, antara lain melalui proses penilaian risiko yang timbul akibat penyediaan jasa TI oleh Bank dan penetapan dasar yang akan digunakan untuk mengidentifikasi pengukuran pengendalian risiko yang memadai.

Tahap pendefinisian kebutuhan di atas harus menghasilkan suatu dokumen yang memuat secara rinci gambaran mengenai paling sedikit:

a. cakupan dan karakteristik dari layanan dan teknologi yang digunakan;
b. jangka waktu, pengakhiran, dan isi minimal dari perjanjian; dan
c. perlindungan perjanjian terhadap kewajiban seperti pembatasan kewajiban, ganti rugi, dan asuransi.

C. Perjanjian Penyediaan Jasa TI oleh Bank

Setelah pendefinisian kebutuhan bisnis penerima jasa TI terhadap penyediaan jasa TI oleh Bank, selanjutnya dalam menyusun perjanjian, Bank harus melalui proses pembahasan dengan satuan kerja hukum dan mempertimbangkan adanya klausul khusus untuk pemutusan perjanjian sebelum berakhirnya perjanjian apabila penerima jasa TI wanprestasi. Klausul khusus memperhatikan antara lain:

1. Pencantuman klausul khusus mengenai kemungkinan mengubah, membuat perjanjian baru, atau menghentikan perjanjian sebelum berakhirnya perjanjian.
2. Bank mampu mengukur risiko dan efisiensi dari penyediaan jasa TI yang dilakukan agar Bank dapat mengetahui secara dini apabila terdapat kondisi-kondisi:

a. memburuknya kondisi Bank akibat penyediaan jasa TI, sehingga berdampak signifikan pada kegiatan usaha Bank;
b. memburuknya kondisi penerima jasa TI, sehingga berdampak signifikan pada kegiatan usaha Bank;
c. tingkat solvabilitas penerima jasa TI tidak memadai, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan; dan/atau
d. terdapat pelanggaran oleh penerima jasa TI terhadap ketentuan peraturan perundang-undangan mengenai kerahasiaan data pribadi nasabah.

3. Dalam hal Bank menemukan hal sebagaimana dimaksud pada angka 2 maka Bank memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penyediaan jasa TI apabila diperlukan.

BAB IX
PENGENDALIAN DAN AUDIT INTERN DALAM PENYELENGGARAAN TI BANK

A. Pengendalian Intern dalam Penyelenggaraan TI

Sistem Pengendalian Intern (SPI) yang efektif merupakan komponen penting dalam Bank dan menjadi dasar bagi kegiatan operasional Bank yang sehat dan aman. SPI yang efektif antara lain dapat membantu Bank dalam menjaga aset Bank, menjamin tersedianya pelaporan keuangan dan manajerial yang dapat dipercaya, serta mengurangi risiko terjadinya kerugian, penyimpangan, dan pelanggaran aspek kehati-hatian.

Dalam penyelenggaraan TI, Bank harus melaksanakan SPI secara efektif terhadap seluruh aspek penggunaan TI.

Dalam rangka pengendalian intern terhadap penyelenggaraan TI, Bank harus memperhatikan hal sebagai berikut:

1. Ketersediaan bukti dan dokumen yang memadai dalam rangka mendukung proses jejak audit (*audit trail*). Proses jejak audit harus dilaksanakan secara efektif dan didokumentasikan untuk memastikan bahwa proses automasi telah bekerja secara efektif dan akurat. Auditor harus melakukan penilaian terhadap efektivitas dan akurasi proses jejak audit ketika melakukan evaluasi atas pelaksanaan pengendalian intern Bank.
2. Pelaksanaan pengendalian terhadap sistem komputer dan pengamanannya (*general controls*) maupun pengendalian terhadap aplikasi perangkat lunak dan prosedur manual lain (*application controls*).
3. Antisipasi terjadinya risiko gangguan atau kerugian yang disebabkan oleh faktor yang berada di luar jangkauan pengendalian rutin Bank sehingga Bank harus menyelenggarakan sistem pemulihan (*recovery*) dan rencana kontinjensi serta pengecekan secara berkala atas kemungkinan terjadinya hal yang sulit diprediksi sebelumnya (*disaster and recovery plan*).
4. Sistem informasi harus menyediakan data dan informasi yang relevan, akurat, tepat waktu, dapat diakses oleh pihak yang berkepentingan, dan disajikan dalam format yang konsisten.
5. Sebagai bagian dari proses pencatatan atau pembukuan, sistem informasi harus didukung oleh sistem akuntansi yang baik termasuk penetapan prosedur dan jadwal retensi pencatatan transaksi.

B. Audit Intern dalam Penyelenggaraan TI

1. Kebijakan, Standar, dan Prosedur terkait Audit TI

Audit intern TI diperlukan untuk melakukan evaluasi terhadap penyelenggaraan TI secara independen dan objektif antara lain untuk meningkatkan efisiensi dan efektivitas manajemen risiko, pengendalian intern, dan tata kelola yang baik.

Sesuai Pasal 54 POJK PTI, Bank melaksanakan fungsi audit intern TI yang efektif dan menyeluruh sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern pada bank umum. Untuk memastikan pelaksanaan audit intern TI, Bank harus memastikan ketersediaan jejak audit (*audit trail*) atas seluruh kegiatan penyelenggaraan TI untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lain.

Bank harus melaksanakan audit intern terhadap seluruh aspek dalam penyelenggaraan TI sesuai kebutuhan, prioritas, dan hasil analisis risiko TI paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Dalam rangka melaksanakan audit TI, Bank harus memiliki kebijakan, standar, dan prosedur yang meliputi:

a. Kebijakan Audit TI

Bank harus memiliki kebijakan audit TI mencakup paling sedikit:

1) tujuan dan latar belakang perlu dilakukannya audit TI;
2) pernyataan independensi terhadap kegiatan operasional dari *auditee*;
3) tanggung jawab auditor terhadap audit TI yang dilakukan secara independen terhadap *auditee*, pelaksanaan *risk assessment* hingga penyelesaian laporan hasil audit;
4) kewenangan auditor dalam melakukan audit TI terhadap akses data, informasi, personel, sistem, dan hal lain yang diperlukan agar audit yang dilakukan dapat berjalan secara efisien dan efektif;
5) tanggung jawab *auditee*, antara lain *system owner*, *data owner, system administrator, security officer, Chief Information Officer*/CIO, terhadap audit TI yang dilakukan, seperti memberikan data, menjalankan rekomendasi, dan perbaikan;
6) batas waktu pemberian data dan tanggapan oleh *auditee*;
7) pernyataan bahwa setiap aktivitas Bank harus masuk dalam ruang lingkup audit TI Bank;
8) tindak lanjut dalam hal terjadi pelanggaran terhadap kebijakan audit TI; dan
9) kaji ulang secara berkala atas fungsi audit intern terhadap penyelenggaraan TI dengan menggunakan jasa pihak ekstern yang independen, sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern pada bank umum.

b. Standar Audit TI

Bank harus memiliki standar audit TI yang mencakup paling sedikit:

1) rencana kerja audit (*Audit Working Plan*/AWP);
2) kertas kerja audit, termasuk hasil atau temuan audit;
3) laporan hasil audit; dan
4) pemantauan tindak lanjut hasil audit.

c. Prosedur Audit TI

Bank harus memiliki prosedur audit TI yang mencakup paling sedikit:

1) tata kelola TI;
2) arsitektur TI;
3) manajemen risiko TI, termasuk pengamanan informasi, jaringan komunikasi, dan Rencana Pemulihan Bencana;
4) penggunaan PPJTI;
5) penempatan Sistem Elektronik;
6) pengelolaan data dan pelindungan data pribadi;
7) penyediaan jasa TI oleh Bank; dan
8) aplikasi bisnis kritikal.

Langkah pemeriksaan disesuaikan dengan masing-masing objek dan cakupan pemeriksaan.

2. Proses Audit TI

Dalam melaksanakan audit TI, terdapat proses yang dijalankan, yaitu:

a. Perencanaan Audit TI

Bank harus memiliki rencana audit TI yang mencakup frekuensi dan jadwal audit TI. Dalam melakukan penilaian risiko, audit intern TI melakukan paling sedikit:

1) mengidentifikasi aset TI, antara lain berupa data (*hardcopy* atau *softcopy*), perangkat lunak, perangkat keras, dan jaringan;
2) mengidentifikasi kegiatan dan proses bisnis yang menggunakan TI;
3) mengidentifikasi tingkat dampak risiko TI dalam operasional Bank; dan
4) mempertimbangkan skala prioritas berdasarkan tingkat risiko.

Rencana audit TI harus mendapat persetujuan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern pada bank umum.

b. Pelaksanaan Audit TI

1) Pelaksanaan audit TI bertujuan untuk:
   a) memastikan kebijakan, standar, dan prosedur penyelenggaraan TI diterapkan secara efektif;
   b) memastikan efektivitas penerapan manajemen risiko TI;
   c) memastikan efektivitas standar pengelolaan informasi dan pengamanan penggunaan TI;
   d) menilai kecukupan kontrol yang diterapkan dalam penyelenggaraan TI;
   e) memberikan rekomendasi perbaikan untuk mengatasi kekurangan dalam penyelenggaraan TI; dan
   f) memastikan kepatuhan penyelenggaraan TI terhadap ketentuan peraturan perundang-undangan.
2) Dalam melaksanakan rencana tahunan audit TI, rencana kerja audit harus disusun untuk setiap penugasan audit, yang mencakup antara lain:
   a) tujuan audit, jadwal, jumlah auditor, anggaran, dan pelaporan;
   b) cakupan audit sesuai hasil penilaian risiko; dan
   c) pembagian tugas dan tanggung jawab dari auditor.
3) Dalam pelaksanaan tugas, auditor TI harus memperhatikan aspek kerahasiaan data dan informasi. Pelaksanaan audit TI harus menggunakan standar kertas kerja pemeriksaan dan didokumentasikan dengan baik. Auditor TI dapat meminta data atau informasi guna keperluan pelaksanaan tugas baik dalam bentuk *hardcopy* maupun *softcopy* termasuk pangkalan data (*database*) dari aplikasi.
4) Auditor TI harus menjunjung tinggi prinsip kode etik (etika) dalam melaksanakan tugas sebagai berikut:
   a) integritas
      (1) bekerja dengan jujur, tekun, dan bertanggung jawab;
      (2) taat terhadap peraturan dan membuat pengungkapan yang sesuai dengan peraturan;

(3) tidak melakukan kegiatan yang ilegal; dan
(4) menghormati dan berperan dalam mendukung tujuan Bank;

b) objektif
(1) tidak ikut berperan dalam kegiatan yang dapat mempengaruhi objektivitas pelaksanaan tugas audit;
(2) tidak menerima apa pun yang dapat mempengaruhi pelaksanaan tugas audit dan bekerja sesuai keahliannya; dan
(3) mengungkapkan fakta sebagaimana yang ditemukan dalam pelaksanaan tugas audit;

c) kerahasiaan
(1) berhati-hati dalam penggunaan data atau informasi dan melindungi data atau informasi dalam pelaksanaan tugas audit; dan
(2) tidak menggunakan data atau informasi untuk kepentingan pribadi ataupun bertentangan dengan hukum; dan

d) kompetensi
(1) memiliki pengetahuan yang memadai;
(2) melaksanakan tugas audit sesuai dengan standar yang ditetapkan oleh Bank; dan
(3) berusaha terus menerus meningkatkan kemampuan untuk meningkatkan kualitas audit.

5) Pernyataan mengenai etika auditor TI tersebut dapat dituangkan dalam bentuk surat pernyataan tertulis yang ditandatangani oleh masing-masing personel auditor TI Bank, termasuk mencakup sanksi apabila yang bersangkutan melanggar etika tersebut.

c. Pelaporan Hasil Audit TI

Laporan hasil audit TI disusun berdasarkan format standar laporan. Laporan tersebut merupakan sarana bagi Bank untuk membantu melakukan penilaian kualitas pengendalian TI. Laporan hasil audit TI harus disampaikan kepada satuan kerja yang diperiksa.

Penyampaian laporan dilakukan secara tepat waktu sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern pada bank umum.

d. Pemantauan Tindak Lanjut Hasil Audit TI

Auditee harus memberikan tanggapan terhadap hasil pemeriksaan. Apabila temuan perlu ditindaklanjuti maka *auditee* harus memberikan komitmen dan target waktu penyelesaiannya. Selanjutnya, auditor TI harus memantau pelaksanaan komitmen *auditee* atas hasil pemeriksaan secara berkala dan melakukan verifikasi terhadap perbaikan yang sudah dilakukan.

Auditor TI harus memelihara dokumentasi atas hasil tindak lanjut tersebut. Laporan hasil pemantauan tindak lanjut perbaikan atas temuan yang signifikan disampaikan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern pada bank umum.

3. Pemenuhan Fungsi Audit Intern TI oleh Auditor Ekstern

Dalam hal terdapat keterbatasan kemampuan satuan kerja audit intern, pelaksanaan fungsi audit intern TI dapat dilakukan oleh

auditor ekstern. Penggunaan auditor ekstern untuk melaksanakan fungsi audit intern atas TI tidak mengurangi tanggung jawab pimpinan satuan kerja audit intern. Selain itu, penggunaan auditor ekstern harus mempertimbangkan ukuran dan kompleksitas usaha Bank serta memperhatikan ketentuan peraturan perundang-undangan terkait auditor ekstern dan pelaksanaannya dilakukan sesuai standar dan prosedur audit TI Bank.
Pelaksanaan fungsi audit intern TI oleh auditor ekstern tetap memperhatikan aspek kompetensi (antara lain pengetahuan dan pengalaman yang memadai) dan independensi serta didasari dengan suatu perjanjian kerja sama. Di samping itu, Bank secara berkala melakukan kaji ulang terhadap fungsi audit intern TI oleh pihak ekstern yang independen agar pelaksanaan fungsi audit TI dapat berjalan efektif.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN II
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

TATA CARA PENYAMPAIAN LAPORAN DAN PERMOHONAN IZIN

A. Penyampaian Informasi dan Pelaporan

1. Rencana Strategis TI

a. Bank menyampaikan RSTI sebagaimana dimaksud dalam Pasal 12 POJK PTI kepada Otoritas Jasa Keuangan dengan memuat dokumen/informasi sesuai dengan Lampiran I Bab III huruf B angka 1.

b. RSTI disampaikan kepada Otoritas Jasa Keuangan paling lambat pada akhir bulan November tahun sebelum periode awal RSTI dimulai.
Contoh:
RSTI periode tahun 2027 sampai dengan tahun 2031 disampaikan kepada Otoritas Jasa Keuangan paling lambat akhir bulan November 2026.

c. Bank dapat melakukan perubahan RSTI dalam hal terdapat kondisi yang secara signifikan memengaruhi sasaran dan strategi TI Bank sebagaimana dimuat dalam RSTI yang sedang berjalan.

d. Bank menyampaikan perubahan RSTI kepada Otoritas Jasa Keuangan sewaktu-waktu dalam periode RSTI, disertai dengan dokumen yang memuat:
   1) alasan perubahan RSTI;
   2) evaluasi kinerja Bank dalam penyelenggaraan TI pada periode sebelum;
   3) visi dan misi Bank terhadap penyelenggaraan TI atau pengkiniannya;
   4) analisis lingkungan internal dan eksternal terkini; dan
   5) sasaran dan strategi Bank terkait penyelenggaraan TI yang terkini.

e. RSTI dan perubahan RSTI disampaikan kepada Otoritas Jasa Keuangan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan.

2. Laporan Rencana Pengembangan TI

a. Sesuai Pasal 58 POJK PTI, Bank wajib melaporkan rencana pengembangan TI. Laporan Rencana Pengembangan TI (LRPTI) merupakan dokumen yang menjabarkan rincian rencana pengembangan TI untuk jangka waktu 1 (satu) tahun ke depan sesuai dengan RSTI Bank.

b. Bank menyampaikan LRPTI kepada Otoritas Jasa Keuangan dengan menggunakan format sebagaimana dimaksud dalam Format 3.1 pada Lampiran III Peraturan Anggota Dewan Komisioner ini.

c. LRPTI disampaikan paling lambat pada akhir bulan November sebelum tahun rencana pengembangan TI.
Contoh:
Bank menyampaikan LRPTI untuk rencana pengembangan TI tahun 2027 paling lambat pada akhir bulan November tahun 2026.

d. LRPTI dapat diubah paling banyak 1 (satu) kali yang disampaikan paling lambat pada akhir bulan Juni tahun berjalan. Perubahan LRPTI dapat diajukan oleh Bank sepanjang memenuhi:
   1) pertimbangan tertentu, antara lain untuk mendukung implementasi kebijakan dan/atau ketentuan di sektor jasa keuangan dan/atau pemerintah untuk mendorong perkembangan perekonomian; dan

2) mendapatkan persetujuan dari Otoritas Jasa Keuangan.

e. Dalam hal terdapat kebutuhan untuk melakukan perubahan atas LRPTI yang berkaitan dengan pengembangan TI atas rencana penyelenggaraan produk bank lanjutan berupa kegiatan berbasis TI, Bank dapat melakukan perubahan terhadap LRPTI paling banyak 3 (tiga) kali dan paling lambat disampaikan pada akhir bulan Maret, bulan Juni, dan bulan September tahun berjalan, sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penyelenggaraan produk Bank.

f. Contoh periode perubahan atas LRPTI sebagaimana dimaksud pada huruf e dapat mengacu pada bagan dalam huruf C Lampiran II ini.

g. Otoritas Jasa Keuangan dapat meminta Bank untuk melakukan penyesuaian terhadap perubahan LRPTI sebagaimana dimaksud pada huruf d dan huruf e.

h. LRPTI dan perubahan LRPTI disampaikan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan.

3. Laporan Kondisi Terkini Penyelenggaraan TI

a. Sesuai Pasal 59 POJK PTI, Bank wajib melaporkan kondisi terkini penyelenggaraan TI. Laporan Kondisi Terkini Penyelenggaraan TI (LKTPTI) berisi kondisi penyelenggaraan TI Bank termasuk perubahan yang telah dilakukan selama 1 (satu) tahun pelaporan.

b. Bank menyampaikan LKTPTI kepada Otoritas Jasa Keuangan dengan menggunakan format sebagaimana dimaksud dalam Format 3.2 pada Lampiran III Peraturan Anggota Dewan Komisioner ini.

c. LKTPTI disampaikan pada setiap tanggal 21 Januari tahun berikutnya, sesuai dengan ketentuan pelaporan bank umum melalui sistem pelaporan Otoritas Jasa Keuangan.
Contoh:
Bank menyampaikan LKTPTI tahun 2027 paling lambat pada tanggal 21 Januari 2028.

d. LKTPTI disampaikan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan.

4. Hasil Kaji Ulang atas Fungsi Audit Intern TI dan Hasil Audit Intern TI

a. Sesuai Pasal 55 ayat (3) POJK PTI, Bank wajib menyampaikan:
1) hasil kaji ulang atas fungsi audit intern TI sebagai bagian dari laporan hasil kaji ulang pihak ekstern yang independen; dan
2) hasil audit intern TI disampaikan sebagai bagian dari laporan pelaksanaan dan pokok-pokok hasil audit intern,
sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern bagi bank umum.

b. Hasil audit intern TI sebagaimana huruf a angka 2) disampaikan kepada Otoritas Jasa Keuangan menggunakan format sebagaimana dimaksud dalam Format 3.3 pada Lampiran III Peraturan Anggota Dewan Komisioner ini.

5. Notifikasi Awal dan Laporan Insiden TI

a. Insiden TI merupakan kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI. Insiden TI terbagi menjadi 2 (dua) kategori yaitu insiden siber dan insiden nonsiber.

b. ketentuan pelaporan insiden TI pada Peraturan Anggota Dewan Komisioner ini berlaku untuk insiden nonsiber. Ketentuan pelaporan bagi insiden siber mengacu pada SEOJK Siber.

c. Dalam hal terjadi insiden nonsiber yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan dan/atau mengganggu kelancaran operasional Bank, Bank wajib menyampaikan:
   1) notifikasi awal insiden TI; dan
   2) laporan insiden TI,

   sesuai dengan Pasal 60 ayat (1) POJK PTI.

d. Notifikasi awal insiden TI disampaikan oleh Bank dengan ketentuan sebagai berikut:
   1) Notifikasi awal disusun menggunakan format sebagaimana tercantum dalam Format 3.4.1 pada Lampiran III Peraturan Anggota Dewan Komisioner ini. Notifikasi awal berisi informasi awal yang tersedia terkait insiden TI pada Bank.
   2) Notifikasi awal disampaikan kepada Otoritas Jasa Keuangan paling lama 24 (dua puluh empat) jam setelah insiden TI diketahui oleh Bank, ditujukan kepada pengawas Bank yang bersangkutan melalui sarana elektronik secara tertulis. Bank melakukan upaya untuk memastikan bahwa notifikasi awal telah diterima oleh Otoritas Jasa Keuangan.

e. Sebagai tindak lanjut dari notifikasi awal insiden TI yang telah disampaikan, Bank melakukan analisis dan penanggulangan insiden TI lebih lanjut. Tindak lanjut ini disampaikan melalui laporan insiden TI kepada Otoritas Jasa Keuangan dengan ketentuan sebagai berikut:
   1) Laporan insiden TI disusun menggunakan format sebagaimana tercantum dalam Format 3.4.2 pada Lampiran III Peraturan Anggota Dewan Komisioner ini. Laporan insiden TI berisi informasi yang lebih lengkap dari informasi yang telah disampaikan pada notifikasi awal.
   2) Laporan insiden TI disampaikan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan paling lama 5 (lima) hari kerja setelah insiden TI diketahui.

f. Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal dan/atau laporan insiden TI, Bank menyampaikan notifikasi awal dan/atau laporan insiden TI kepada Otoritas Jasa Keuangan dengan ketentuan sebagai berikut:
   1) Dalam hal otoritas lain mengatur jangka waktu penyampaian notifikasi awal dan/atau laporan insiden TI lebih cepat dari jangka waktu sebagaimana diatur dalam POJK PTI maka Bank menyampaikan notifikasi awal dan/atau laporan insiden TI kepada Otoritas Jasa Keuangan pada saat yang bersamaan sesuai dengan ketentuan peraturan perundang-undangan dari otoritas lain dimaksud.

Contoh:
Ketentuan Otoritas "ABC"

a) Jangka waktu penyampaian notifikasi awal disampaikan paling lama 1 (satu) jam setelah insiden TI diketahui.
b) Jangka waktu penyampaian laporan insiden TI disampaikan paling lama 3 (tiga) hari kerja setelah insiden siber diketahui.

Bank "X" mengalami insiden TI pada tanggal 2 Januari 2026 pukul 13.00 WITA. Mengingat jangka waktu penyampaian notifikasi awal dan/atau laporan insiden TI berdasarkan ketentuan Otoritas "ABC" lebih cepat daripada yang diatur dalam ketentuan Otoritas Jasa Keuangan, maka Bank "X" menyampaikan notifikasi awal dalam kurun waktu 1 (satu) jam setelah insiden TI diketahui. Apabila Bank "X" menyampaikan notifikasi awal insiden TI kepada Otoritas "ABC" pada pukul 13.45 WITA maka Bank "X" juga menyampaikan notifikasi awal kepada Otoritas Jasa Keuangan pada saat yang bersamaan.

Hal yang sama juga berlaku untuk penyampaian laporan insiden TI. Apabila Bank "X" menyampaikan laporan insiden TI pada tanggal 4 Januari 2026 pukul 10.00 WITA kepada Otoritas "ABC" maka Bank "X" juga menyampaikan laporan insiden TI kepada Otoritas Jasa Keuangan pada saat yang bersamaan.

2) Apabila otoritas lain mengatur jangka waktu penyampaian notifikasi awal dan/atau laporan insiden TI lebih lama dari jangka waktu sebagaimana diatur dalam POJK PTI, maka Bank menyampaikan notifikasi awal dan/atau laporan insiden TI kepada Otoritas Jasa Keuangan sesuai dengan POJK PTI.

Contoh:
Ketentuan Otoritas "DEF"

a) Jangka waktu penyampaian notifikasi awal disampaikan paling lama 3 (tiga) hari kerja setelah insiden siber diketahui.
b) Jangka waktu penyampaian laporan insiden TI disampaikan paling lama 10 (sepuluh) hari kerja setelah insiden siber diketahui.

Bank "Y" mengalami insiden siber pada tanggal 2 Januari 2026 pukul 13.00 WITA. Mengingat jangka waktu penyampaian notifikasi awal dan/atau laporan insiden TI berdasarkan ketentuan Otoritas Jasa Keuangan lebih cepat daripada yang diatur dalam ketentuan Otoritas "DEF", maka Bank "Y" menyampaikan notifikasi awal kepada Otoritas Jasa Keuangan dalam kurun waktu 24 (dua puluh empat) jam setelah insiden TI diketahui.

Hal yang sama juga berlaku untuk penyampaian laporan insiden TI. Bank "Y" menyampaikan laporan insiden TI dalam kurun waktu 5 (lima) hari kerja setelah insiden TI diketahui kepada Otoritas Jasa Keuangan.

B. Perizinan dan Laporan Realisasi

1. Perizinan

a. Bank yang akan menyelenggarakan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia, harus mengajukan permohonan izin kepada Otoritas Jasa Keuangan. Dalam mengajukan permohonan izin, Bank harus memenuhi Pasal 35, Pasal 36, dan Pasal 37 POJK PTI. Permohonan izin tersebut disertai dengan dokumen sebagaimana tercantum dalam Format 4.1 pada Lampiran IV Peraturan Anggota Dewan Komisioner ini.

b. Bank yang akan menyerahkan penyelenggaraan pemrosesan transaksi berbasis TI kepada pihak penyedia jasa di luar wilayah Indonesia, harus mengajukan permohonan izin kepada Otoritas Jasa Keuangan. Dalam mengajukan permohonan izin, Bank harus memenuhi Pasal 39 POJK PTI. Permohonan izin tersebut disertai dengan dokumen sebagaimana tercantum dalam Format 4.3 pada Lampiran IV Peraturan Anggota Dewan Komisioner ini.

c. Bank yang memiliki rencana sebagai penyedia jasa TI harus mengajukan permohonan izin kepada Otoritas Jasa Keuangan. Dalam mengajukan permohonan izin, Bank harus memenuhi Pasal 48 POJK PTI. Permohonan izin tersebut disertai dengan dokumen sebagaimana tercantum dalam Format 4.5 pada Lampiran IV Peraturan Anggota Dewan Komisioner ini.

d. Permohonan izin sebagaimana dimaksud pada huruf a, huruf b, dan huruf c disampaikan kepada Otoritas Jasa Keuangan secara daring sesuai dengan Pasal 40 ayat (1) POJK PTI, melalui sistem perizinan dan registrasi terintegrasi Otoritas Jasa Keuangan.

e. Dalam hal sarana penyampaian sebagaimana dimaksud pada huruf d belum tersedia, penyampaian dilakukan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan dengan alamat https://sipenaojk.ojk.go.id, dengan tujuan kepada:
   1) Departemen Pengawasan Bank terkait atau Kantor Regional Otoritas Jasa Keuangan di Jakarta, bagi Bank yang berkantor pusat di wilayah Provinsi Daerah Khusus Ibukota Jakarta atau Provinsi Banten; atau
   2) Kantor Regional Otoritas Jasa Keuangan atau Kantor Otoritas Jasa Keuangan setempat, bagi Bank yang berkantor pusat di luar wilayah Provinsi Daerah Khusus Ibukota Jakarta atau Provinsi Banten.

f. Dalam hal sarana penyampaian sebagaimana dimaksud pada huruf e tidak tersedia, penyampaian dilakukan secara daring melalui layanan *mailing room* Otoritas Jasa Keuangan.

g. Otoritas Jasa Keuangan memberikan izin atau menolak permohonan izin:
   1) penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 35 POJK PTI; atau
   2) pemrosesan transaksi berbasis TI oleh PPJTI di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 39 POJK PTI,

   paling lama 3 (tiga) bulan setelah seluruh persyaratan dipenuhi oleh Bank dan dokumen permohonan diterima secara lengkap oleh Otoritas Jasa Keuangan.

2. Laporan Realisasi

a. Bank harus menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud pada angka 1 huruf a.

b. Bank harus mengimplementasikan pemrosesan transaksi berbasis TI oleh PPJTI di luar wilayah Indonesia sebagaimana dimaksud pada angka 1 huruf b.

c. Bank harus melaksanakan rencana penyediaan jasa TI sebagaimana dimaksud pada angka 1 huruf c.

d. Apabila Bank tidak melakukan realisasi sebagaimana dimaksud pada huruf a, huruf b, dan huruf c dalam jangka waktu 6 (enam) bulan sejak izin diperoleh dari Otoritas Jasa Keuangan, izin Otoritas Jasa Keuangan menjadi tidak berlaku.

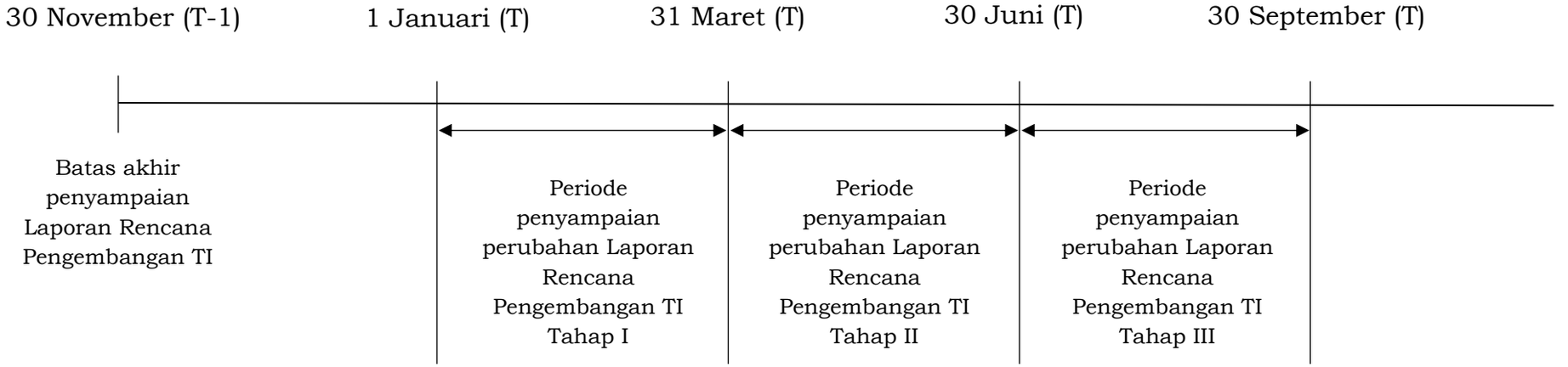
e. Bank menyampaikan laporan realisasi atas penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud pada angka 1 huruf a dengan menggunakan format sebagaimana dimaksud dalam Format 4.2 pada Lampiran IV Peraturan Anggota Dewan Komisioner ini.

f. Bank menyampaikan laporan realisasi atas implementasi pemrosesan transaksi berbasis TI oleh PPJTI di luar wilayah Indonesia sebagaimana dimaksud pada angka 1 huruf b dengan menggunakan format sebagaimana dimaksud dalam Format 4.4 pada Lampiran IV Peraturan Anggota Dewan Komisioner ini.

g. Bank menyampaikan laporan realisasi atas pelaksanaan rencana penyediaan jasa TI sebagaimana dimaksud pada angka 1 huruf c dengan menggunakan format sebagaimana dimaksud dalam Format 4.6 pada Lampiran IV Peraturan Anggota Dewan Komisioner ini.

h. Laporan realisasi sebagaimana dimaksud pada huruf e, huruf f, dan huruf g disampaikan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan dengan alamat https://sipenaojk.ojk.go.id paling lama 3 (tiga) bulan setelah implementasi.

C. Bagan Alur Waktu Penyampaian Laporan Rencana Pengembangan TI dalam Rangka Penyelenggaraan Produk Bank Lanjutan berupa Kegiatan Berbasis TI



Keterangan:

(1) T = Tahun rencana penyelenggaraan TI yang terkait dengan produk Bank lanjutan berupa kegiatan berbasis TI.

(2) Bank hanya dapat melakukan perubahan Laporan Rencana Pengembangan TI paling banyak 1 (satu) kali pada setiap tahap.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN III
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

FORMAT LAPORAN DAN NOTIFIKASI

DAFTAR ISI

Format 3.1

LAPORAN RENCANA PENGEMBANGAN TEKNOLOGI INFORMASI

No.	Nama Aplikasi/ Infrastruktur Bank	Deskripsi	Kategori	Jenis Pengembangan	Pengembang	PPJTI Pihak Terkait	Lokasi		Waktu Rencana Implementasi	Estimasi Biaya		Ket.
							Pusat Data	Pusat Pemulihan Bencana		Biaya Investasi	Biaya Operasional	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)		(9)	(10)		(11)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan nama aplikasi/ infrastruktur yang akan dikembangkan. Contoh: "Aplikasi X", "Relokasi Pusat Data", "Penambahan kapasitas *bandwidth* jaringan".
(3) Penjelasan detail aplikasi/infrastruktur yang dikembangkan.
(4) Kategori pengembangan, pilih salah satu:
- 01 : Pengelolaan nasabah
- 02 : Dana pihak ketiga (giro, tabungan, deposito)
- 03 : Perkreditan/pembiayaan
- 04 : Buku Besar (*General Ledger*/GL)
- 05 : Pembayaran
- 06 : Layanan Digital
- 07 : Tresuri
- 08 : Pembiayaan Perdagangan (*Trade finance*)
- 09 : APU-PPT dan PPPSPM
- 10 : Manajemen sistem informasi pelaporan
- 11 : Manajemen risiko
- 12 : Manajemen intern
- 49 : Aplikasi lain
- 51 : Pusat Data/Pusat Pemulihan Bencana
- 52 : Server dan/atau platform
- 53 : Jaringan komunikasi data
- 54 : Sistem keamanan (*security system*)
- 99 : Infrastruktur lain

(5) Diisi "baru" jika aplikasi/infrastruktur baru atau mengganti aplikasi/infrastruktur yang lama, diisi "*upgrade*" untuk penambahan/pengembangan terhadap aplikasi/infrastruktur yang telah ada.
(6) Diisi "*inhouse*" jika dikembangkan oleh pihak internal Bank atau diisi "PPJTI" jika dikembangkan oleh pihak eksternal Bank.
(7) Diisi "ya" jika PPJTI merupakan pihak terkait Bank, "tidak" jika PPJTI bukan merupakan pihak terkait, "-" jika pengembangan dilakukan secara *inhouse* atau PPJTI belum ditetapkan.
(8) Diisi informasi nama kota dan negara lokasi Pusat Data dan Pusat Pemulihan Data.
(9) Diisi menggunakan periode triwulan yaitu TW1/TW2/TW3/TW4.
(10) Diisi estimasi Biaya Investasi (*capex*) dan/atau Biaya Operasional (*opex*) selama 1 (satu) tahun sejak implementasi (tidak termasuk biaya penyusutan *capex*). Biaya dalam satuan mata uang Rupiah atau satuan mata uang lain disertai dengan nilai ekuivalen dalam mata uang Rupiah.
(11) Diisi dengan, antara lain:
- dampak-dampak pengembangan TI, misalnya butuh penambahan SDM.
- penjelasan keterkaitan pengembangan TI dengan RSTI.
- keterkaitan dengan rencana penyelenggaraan produk bank baru (RPPB) sesuai POJK mengenai penyelenggaraan produk Bank.

Format 3.2

LAPORAN KONDISI TERKINI PENGGUNAAN TEKNOLOGI INFORMASI

DAFTAR DOKUMEN DAN INFORMASI DALAM LAPORAN KONDISI TERKINI PENGGUNAAN TEKNOLOGI INFORMASI

No.	Nama Dokumen atau Informasi
1	Informasi Pelapor
2	Organisasi dan Manajemen
2.1	Struktur Organisasi Bank dan Jumlah Sumber Daya Manusia Bank
2.2	Struktur Organisasi TI dan Jumlah Sumber Daya Manusia TI
2.3	Surat Keputusan Komite Pengarah TI Terkini
2.4	Risalah Rapat Komite Pengarah TI 1 (satu) Tahun Terakhir
3	Kebijakan, Standar, dan Prosedur TI
4	Manajemen Risiko
4.1	Penerapan Manajemen Risiko
4.2	Struktur Organisasi Audit Intern TI
4.3	Audit TI 1 (satu) Tahun Terakhir
5	Arsitektur TI
6	Daftar Aplikasi
7	Terminal Perbankan Elektronik
8	Pusat Data (*Data Centre*) dan Pusat Pemulihan Bencana (*Disaster Recovery Centre*)
9	Pengamanan TI
10	Rencana Pemulihan Bencana (*Disaster Recovery Plan*)
11	Penyedia Jasa TI
12	Biaya TI
13	Penilaian terkait Keamanan Siber Bank
13.1	Kertas Kerja Penilaian Risiko Inheren terkait Keamanan Siber
13.2	Hasil Penilaian terkait Keamanan Siber Bank
13.3	Kerta Kerja Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber
13.4	Kerta Kerja Penilaian Kualitas Penerapan Proses Ketahanan Siber
14	Hasil Pengujian Keamanan Siber berdasarkan Analisis Kerentanan
15	Penilaian Sendiri atas Tingkat Maturitas Digital
15.1	Kertas Kerja Penilaian Kualitas Penerapan Aspek Maturitas Digital Bank
15.2	Hasil Penilaian Tingkat Maturitas Digital Bank
16	Daftar Mitra Bank dalam Melakukan Kerja Sama Layanan Digital
17	Hasil Identifikasi Sistem Elektronik

Format 3.2.1

INFORMASI PELAPOR

Nama Bank : .....
Alamat Kantor Pusat Bank : .....
Nomor Telepon : .....
Nama Narahubung : .....
Nomor Telepon Narahubung : .....
Kantor/Divisi/Bagian Pelapor: .....
Alamat Kantor/Divisi/Bagian Pelapor: .....
Tanggal Pelaporan: ..../..../..... (*dd/mm/yyyy*)

Format 3.2.2

ORGANISASI DAN MANAJEMEN

Nomor Format	Deskripsi Informasi	Keterangan
2.1	Struktur Organisasi Bank dan Jumlah SDM Bank	*(dilampirkan)*
2.2	Struktur Organisasi TI dan Jumlah SDM TI	*(dilampirkan)*
2.3	Surat Keputusan Komite Pengarah TI Terkini	*(dilampirkan)*
2.4	Risalah Rapat Komite Pengarah TI 1 (satu) Tahun Terakhir	*(dilampirkan)*

Format 3.2.3

KEBIJAKAN, STANDAR, DAN PROSEDUR TEKNOLOGI INFORMASI

No.	Nomor Dokumen	Judul Dokumen	Deskripsi	Kategori	Jenis	Revisi Terakhir
(1)	(2)	(3)	(4)	(5)	(6)	(7)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan nomor dokumen versi Bank.
(3) Diisi dengan judul dokumen.
(4) Diisi keterangan singkat mengenai isi dari dokumen, contoh: kebijakan pemilihan PPJTI dalam hal calon PPJTI merupakan pihak terkait.
(5) Diisi dengan salah satu kategori:
- 300 : Tata Kelola TI (termasuk Organisasi dan Manajemen)
- 301 : Manajemen Risiko
- 302 : Pengembangan dan Pengadaan
- 303 : Operasional TI
- 304 : Jaringan Komunikasi
- 305 : Pengamanan Informasi
- 306 : Rencana Pemulihan Bencana
- 307 : Penggunaan PPJTI
- 308 : Penyediaan Jasa TI oleh Bank
- 309 : Ketahanan dan Keamanan TI termasuk siber
- 310 : Pengelolaan Data
- 311 : Pengendalian Intern
- 312 : Lainnya

(6) Diisi dengan salah satu jenis:
K = Kebijakan
S = Standar
P = Prosedur
(7) Diisi tanggal revisi terakhir (*dd-mm-yyyy*).

Format 3.2.4

MANAJEMEN RISIKO

4.1 PENERAPAN MANAJEMEN RISIKO

Kecukupan kebijakan, standar, dan prosedur penggunaan TI	..... (Penjelasan singkat mengenai kebijakan, standar, dan prosedur penggunaan TI)
Kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko penggunaan TI	..... (Penjelasan singkat mengenai proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko penggunaan TI)
Sistem pengendalian intern atas penggunaan TI	..... (Penjelasan singkat mengenai mekanisme pengendalian risiko dan hasilnya)
IT *Risk Rating* (*Low*, *Low-to-moderate*, *Moderate*, *Moderate-to-high*, *High*)	..... (Nilai akhir *self asessment* IT *risk rating*)

4.2 STRUKTUR ORGANISASI AUDIT INTERN TEKNOLOGI INFORMASI

(Diisi dengan gambar Struktur Organisasi Audit Intern TI; Sebutkan jumlah SDM Satuan Kerja Audit Intern-TI)

4.3 AUDIT TEKNOLOGI INFORMASI 1 (SATU) TAHUN TERAKHIR

Periode Audit	Jenis Audit	Cakupan Audit
(1)	(2)	(3)

Keterangan:
(1) Diisi tanggal mulai dan tanggal selesai audit.
(2) Diisi jenis audit: intern atau ekstern.
(3) Diisi cakupan audit (contoh: Modul pinjaman *core banking system*).

Format 3.2.5

ARSITEKTUR TI

Arsitektur Data
(Diisi dengan diagram Arsitektur Data)

Arsitektur Aplikasi
(Diisi dengan diagram Arsitektur Aplikasi)

Arsitektur Teknologi
(Diisi dengan diagram Arsitektur Teknologi)

*) Diagram Arsitektur TI disesuaikan dengan kompleksitas bisnis Bank. Diagram arsitektur TI menggambarkan kondisi terkini TI Bank pada saat periode pelaporan.

Format 3.2.6

DAFTAR APLIKASI

No.	Kategori Aplikasi	Nama Aplikasi	Deskripsi Fungsi Aplikasi	*Platform*	Pangkalan Data	Lokasi				Strategi *Backup*	*System Owner*	Pengembang Aplikasi (*inhouse*/ Pihak Penyedia Jasa TI)	Tanggal Implementasi (*Go Live*)	Kepemilikan (Sewa atau Beli Putus)
						DC	Penyeleng-gara DC	DRC	Penyeleng-gara DRC					
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan salah satu kategori:
- 01 : Pengelolaan nasabah
- 02 : Dana pihak ketiga (giro, tabungan, deposito)
- 03 : Perkreditan/pembiayaan
- 04 : Buku Besar (*General Ledger*/GL)
- 05 : Pembayaran
- 06 : Layanan Digital
- 07 : Tresuri
- 08 : Pembiayaan Perdagangan (*Trade finance*)
- 09 : APU-PPT dan PPPSPM
- 10 : Manajemen sistem informasi pelaporan
- 11 : Manajemen risiko
- 12 : Manajemen intern
- 49 : Aplikasi lain

(3) Diisi dengan nama aplikasi.
(4) Diisi dengan keterangan singkat mengenai fungsi aplikasi.
(5) Diisi platform sistem operasi.
(6) Diisi *database engine* yang diperlukan.
(7) Diisi dengan kota dan/atau negara lokasi Pusat Data.
(8) Diisi dengan nama perusahaan Penyelenggara DC atau “sendiri” (Bank).
(9) Diisi kota dan/atau negara lokasi Pusat Pemulihan Bencana aplikasi.

(10) Diisi perusahaan Penyelenggara DRC atau “sendiri” (Bank).
(11) Diisi:
- *High Availability Active - Active*
- *High Availability Active - Passive*
- *Backup Realtime*
- *Backup Periodically*

(12) Diisi unit bisnis yang mengelola aplikasi.
(13) Diisi:
- “*inhouse”*, jika aplikasi dikembangkan sendiri oleh Bank.
- Nama PPJTI, jika aplikasi dikembangkan oleh PPJTI.

(14) Diisi dengan tanggal implementasi aplikasi (*dd-mm-yyyy*).
(15) Diisi “Sewa” atau “Beli Putus”.

Format 3.2.7

TERMINAL PERBANKAN ELEKTRONIK

No.	Nama TPE	Jenis TPE	Jumlah	Frekuensi Transaksi	Nominal Transaksi per Tahun	Jumlah Pengguna
(1)	(2)	(3)	(4)	(5)	(6)	(7)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan nama dari produk atau *platform* terminal perbankan elektronik (TPE), jika ada. Contoh: "*A Bank Mobile*"
(3) Diisi dengan salah satu jenis TPE:
- Anjungan Tunai Mandiri (ATM);
- *Cash Deposit Machine* (CDM);
- *Cash Recycler Machine* (CRM);
- *Electronic Data Capture* (EDC);
- *Phone Banking*;
- *SMS Banking*;
- *Internet/ Mobile Banking*;
- Lainnya (dapat diisi dengan: uang elektronik atau dompet elektronik).

(4) Diisi dengan jumlah unit TPE.
(5) Diisi dengan jumlah frekuensi transaksi dari TPE.
(6) Diisi dengan jumlah nominal transaksi dari TPE selama 1 (satu) tahun laporan.
(7) Diisi dengan jumlah pengguna TPE, jika ada.

Format 3.2.8

PUSAT DATA (*DATA CENTER*/DC) DAN PUSAT PEMULIHAN BENCANA (*DISASTER RECOVERY CENTER*/DRC)

DC/DRC 1	
Keterangan	
Fungsi :	*(Diisi "DC" atau "DRC")*
Penyelenggara :	*(Diisi "sendiri" (Bank) atau nama penyelenggara)*
Alamat dan/atau Lokasi:	*(Diisi dengan alamat dari DC atau DRC)*
Luas Area DC/DRC:*)	*(Diisi dengan luas area DC atau DRC)*
Sertifikasi DC/DRC:	*(Hasil penilaian sesuai sertifikasi jika ada/ekuivalen berdasarkan assessment intern)*
Pengendalian fisik: *) *Contoh:* *- Pintu Pusat Data dan Pusat Pemulihan Bencana harus selalu terkunci dan dilengkapi dengan kartu akses dan/atau biometric device* *- Ruang Pusat Data dan Pusat Pemulihan Bencana tidak boleh diberi label atau papan petunjuk (signing board) agar orang tidak mudah mengenali* *- Bank harus memiliki log-book untuk mencatat tamu yang memasuki Pusat Data dan Pusat Pemulihan Bencana* *- Menjaga privasi lokasi Pusat Data dan Pusat Pemulihan Bencana*	*(Penjelasan singkat mengenai pengendalian fisik di DC/DRC)*
Pengendalian lingkungan: *) *Contoh:* *- Uninterruptible Power Supply (UPS)* *- Lantai yang ditinggikan (raised floor)* *- Pengaturan suhu dan kelembaban udara (AC, termometer, dan higrometer)* *- Pendeteksi asap/api/panas/kebocoran air* *- Sistem pemadaman api* *- Kamera CCTV* *- dan lain-lain*	..... *(Penjelasan singkat mengenai pengendalian lingkungan di DC/DRC)*

DC/DRC – 2, 3, ...	
Keterangan	
Fungsi :	*(Diisi "DC" atau "DRC")*
Penyelenggara :	*(Diisi "sendiri" (Bank) atau nama penyelenggara)*
Alamat dan/atau Lokasi:	*(Diisi dengan alamat dari DC atau DRC)*
Luas Area DC/DRC:*)	*(Diisi dengan luas area DC atau DRC)*

Sertifikasi DC/DRC:	*(Hasil penilaian sesuai sertifikasi jika ada/ekuivalen berdasarkan assessment intern)*
Pengendalian fisik: *) *Contoh:* *- Pintu Pusat Data dan Pusat Pemulihan Bencana harus selalu terkunci dan dilengkapi dengan kartu akses dan/atau biometric device* *- Ruang Pusat Data dan Pusat Pemulihan Bencana tidak boleh diberi label atau papan petunjuk (signing board) agar orang tidak mudah mengenali* *- Bank harus memiliki log-book untuk mencatat tamu yang memasuki Pusat Data dan Pusat Pemulihan Bencana* *- Menjaga privasi lokasi Pusat Data dan Pusat Pemulihan Bencana*	*(Penjelasan singkat mengenai pengendalian fisik di DC/DRC)*
Pengendalian lingkungan: *) *Contoh:* *- Uninterruptible Power Supply (UPS)* *- Lantai yang ditinggikan (raised floor)* *- Pengaturan suhu dan kelembaban udara (AC, termometer, dan higrometer)* *- Pendeteksi asap/api/panas/kebocoran air* *- Sistem pemadaman api* *- Kamera CCTV* *- dan lain-lain*	..... *(Penjelasan singkat mengenai pengendalian lingkungan di DC/DRC)*

Keterangan:
*) hanya diisi jika DC/DRC diselenggarakan secara mandiri oleh Bank (*on premise*).

Format 3.2.9

PENGAMANAN TEKNOLOGI INFORMASI

No.	Nama Aset	Tipe Aset	Deskripsi
(1)	(2)	(3)	(4)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan nama aset untuk pengamanan TI (contoh: antivirus "XYZ" dan firewall "ABC").
(3) Diisi dengan jenis aset (*software* atau *hardware*).
(4) Diisi dengan keterangan singkat mengenai aset (seperti fungsi aset, jumlah lisensi, versi aset, dan lain-lain).

Format 3.2.10

RENCANA PEMULIHAN BENCANA (*DISASTER RECOVERY PLAN*/DRP)

A. Informasi Umum DRP

Jenis	: *(Diisi dengan informasi umum mengenai jenis)*
Lokasi media rekam cadang (backup)	*: (Diisi dengan lokasi media rekam cadang (backup))*
Tanggal pengujian DRP terakhir	*: (Diisi waktu pengujian DRP)*

B. Struktur Tim DRP

(Diisi dengan gambar Struktur Tim DRP)

C. Pengujian DRP

Pengujian DRP – 1	
Waktu Pengujian	*(Diisi waktu pengujian DRP)*
Daftar Aplikasi dan/atau Infrastruktur Bank	*(Diisi daftar aplikasi dan/atau infrastruktur yang diuji dalam 1 (satu) tahun terakhir)*
Hasil Pengujian dari DRP	*(Diisi penjelasan singkat mengenai hasil pengujian DRP)*

Pengujian DRP – 2, 3, ...	
Waktu Pengujian	*(Diisi waktu pengujian DRP)*
Daftar Aplikasi dan/atau Infrastruktur Bank	*(Diisi daftar aplikasi dan/atau infrastruktur yang diuji dalam 1 (satu) tahun terakhir)*
Hasil Pengujian dari DRP	*(Diisi penjelasan singkat mengenai hasil pengujian DRP)*

D. Pelaksanaan Kaji Ulang DRP

Pelaksanaan Kaji Ulang DRP - 1	
Waktu Pelaksanaan Kaji Ulang 1	*(Diisi waktu kaji ulang DRP)*
Waktu Pelaksanaan Kaji Ulang 2 (jika ada)	*(Diisi waktu kaji ulang DRP)*
Daftar Aplikasi dan/atau Infrastruktur Bank	*(Diisi daftar aplikasi dan/atau infrastruktur yang dikaji ulang dalam 1 (satu) tahun terakhir)*
Hasil Kaji Ulang	*(Diisi dengan hasil kaji ulang)*
Pelaksana Kaji Ulang	*(Diisi dengan jabatan dan nama petugas yang melakukan kaji ulang)*
Tindak Lanjut Kaji Ulang	*(Diisi dengan langkah-langkah yang perlu diambil setelah pelaksanaan kaji ulang)*

Pelaksanaan Kaji Ulang DRP – 2, 3, ...	
Waktu Pelaksanaan Kaji Ulang 1	*(Diisi waktu kaji ulang DRP)*

Waktu Pelaksanaan Kaji Ulang 2 (jika ada)	*(Diisi waktu kaji ulang DRP)*
Daftar Aplikasi dan/atau Infrastruktur Bank	*(Diisi daftar aplikasi dan/atau infrastruktur yang dikaji ulang dalam 1 (satu) tahun terakhir)*
Hasil Kaji Ulang	*(Diisi dengan hasil kaji ulang)*
Pelaksana Kaji Ulang	*(Diisi dengan jabatan dan nama petugas yang melakukan kaji ulang)*
Tindak Lanjut Kaji Ulang	*(Diisi dengan langkah-langkah yang perlu diambil setelah pelaksanaan kaji ulang)*

Format 3.2.11

PENYEDIA JASA TEKNOLOGI INFORMASI

A. Penggunaan Pihak Penyedia Jasa TI oleh Bank

No.	Nama PPJTI	Alamat PPJTI	Pihak Terkait	Jasa TI yang Diberikan	Tanggal Dimulai Kerja Sama
(1)	(2)	(3)	(4)	(5)	(6)

B. Bank sebagai Penyedia Jasa TI

No.	Nama Pengguna Jasa TI	Alamat Pengguna Jasa TI	Pihak Terkait	Jasa TI yang Diberikan	Tanggal Dimulai Kerja Sama
(1)	(2)	(3)	(4)	(5)	(6)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan nama PPJTI atau nama pengguna jasa TI Bank.
(3) Diisi dengan alamat PPJTI atau alamat pengguna jasa TI Bank.
(4) Diisi:
- "Y", jika PPJTI atau pengguna jasa TI Bank merupakan pihak terkait dengan Bank; atau
- "T", jika PPJTI atau pengguna jasa TI Bank bukan merupakan pihak terkait dengan Bank.

(5) Diisi dengan daftar jasa TI yang diberikan PPJTI kepada Bank atau jasa TI yang diberikan oleh Bank kepada pengguna, seperti:
- Penyelenggaraan Pusat Data;
- Penyelenggaraan Pusat Pemulihan Bencana; dan
- Penyediaan layanan aplikasi.

(6) Diisi dengan tanggal dimulainya kerja sama antara Bank dan PPJTI, atau antara Bank dan pengguna jasa TI.

Format 3.2.12

BIAYA TEKNOLOGI INFORMASI

Jenis Biaya	Kepada pihak terkait *)	Kepada pihak tidak terkait*)
1. Pembebanan ke laba/rugi		
a. Biaya modal yang dapat dikapitalisasikan (*capital expenditure*/c*apex*)		
b. Biaya operasional (*operational expenditure*/*opex*)		
2. Pembebanan ke neraca		

Keterangan:
(1.a) Diisi dengan penyusutan biaya investasi (*capex*) ke laba/rugi.
(1.b) Diisi dengan pembebanan biaya operasional (*opex*) ke laba/rugi.
(2) Diisi dengan tambahan biaya investasi (*capex*) tahun berjalan ke neraca.

*) Biaya dalam satuan mata uang Rupiah atau satuan mata uang lain disertai dengan nilai ekuivalen dalam mata uang Rupiah.

Format 3.2.13

PENILAIAN TERKAIT KEAMANAN SIBER BANK

Nomor Format	Nama Informasi/Laporan	Keterangan
13.1	Kertas Kerja Penilaian Risiko Inheren terkait Keamanan Siber	*(dilampirkan)*
13.2	Hasil Penilaian terkait Keamanan Siber Bank	*(dilampirkan)*
13.3	Kertas Kerja Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber	*(dilampirkan)*
13.4	Kertas Kerja Penilaian Kualitas Penerapan Proses Ketahanan Siber	*(dilampirkan)*

Keterangan:
Seluruh format laporan dan informasi penilaian terkait keamanan siber Bank disampaikan sesuai dengan SEOJK Siber.

Format 3.2.14

HASIL PENGUJIAN KEAMANAN SIBER
BERDASARKAN ANALISIS KERENTANAN

A. Informasi Ruang Lingkup Pengujian
1. Jenis aset yang diuji, termasuk lingkungannya (*development* atau *production*)
2. Tujuan pengujian dan metode pengujian (*white box*, *black box* atau *grey box*)

B. Informasi Temuan
1. Penjelasan terkait dengan temuan dan tingkat kritikalitasnya
2. Ringkasan dampak temuan terhadap kelangsungan bisnis Bank

C. Status Tindak Lanjut Temuan

D. Informasi Pendukung Lain *(dilampirkan)*

Format 3.2.15

PENILAIAN SENDIRI ATAS TINGKAT MATURITAS DIGITAL

Nomor Format	Nama Informasi/Laporan	Keterangan
15.1	Kertas Kerja Penilaian Kualitas Penerapan Aspek Maturitas Digital Bank	*(dilampirkan)*
15.2	Hasil Penilaian Tingkat Maturitas Digital Bank	*(dilampirkan)*

Keterangan:
Seluruh format laporan dan informasi disampaikan sesuai dengan SEOJK DMAB.

Format 3.2.16

DAFTAR MITRA BANK
DALAM MELAKUKAN KERJA SAMA LAYANAN DIGITAL

No.	Nama Mitra Bank*)	Jenis Layanan Digital*)
(1)	(2)	(3)

Keterangan:
(1) Diisi dengan nomor urut.
(2) Diisi dengan nama perusahaan mitra Bank.
(3) Diisi dengan jenis layanan (contoh: pembukaan rekening, informasi saldo, pemasaran produk).

*) Yang dimaksud dengan mitra Bank yaitu perusahaan yang bekerja sama dengan Bank dalam penyelenggaraan layanan digital sesuai dengan POJK mengenai layanan digital oleh bank umum.

Format 3.2.17

HASIL IDENTIFIKASI SISTEM ELEKTRONIK

A. Informasi Umum

Profil Bank Umum		
1	Nama Bank	: *(diisi dengan nama perusahaan Bank)*
2	Tahun	: *(diisi dengan tahun pelaksanaan identifikasi)*
3	Alamat Bank	: *(diisi dengan alamat kantor pusat Bank)*
4	Daftar fungsi, layanan atau proses bisnis yang dijalankan	: *(diisi dengan kegiatan usaha yang dilakukan, contoh: menyalurkan dana pihak ketiga, menghimpun dana pihak ketiga, melakukan sistem pembayaran)*
5	Jumlah pengguna akhir yang dilayani	: *(dapat diisi dengan data total CIF)*
6	Populasi terpengaruh layanan	: *(dapat diisi dengan data total rekening nasabah)*

Kontak Narahubung		
7	Nama Narahubung	: *(diisi dengan nama pegawai yang bertugas sebagai narahubung dari pelaksanaan identifikasi)*
8	Satuan Kerja Narahubung	: *(diisi dengan satuan/unit kerja dari pegawai yang menjadi narahubung)*
9	Kontak Telepon Narahubung	: a. Telepon : *(diisi dengan nomor telepon kantor dari narahubung)* b. Telepon seluler : *(diisi dengan nomor telepon dari narahubung)* c. Email : *(diisi dengan alamat email resmi dari narahubung)*

Keterangan:
Informasi hasil identifikasi Sistem Elektronik disampaikan dalam rangka memenuhi ketentuan peraturan perundang-undangan mengenai infrastruktur informasi vital.

B. Identifikasi Sistem Elektronik terkait Infrastruktur Informasi Vital

No.	Jenis Sistem Elektronik	Nama Sistem Elektronik	Layanan Sistem Elektronik	Daftar Data yang Dikelola	Hubungan Ketergantungan dan Penggunaan Pihak Ketiga	Rencana Keberlangsungan Layanan
(1)	(2)	(3)	(4)	(5)	(6)	(7)

Kategori Sistem Elektronik	Hasil Pengukuran Tingkat Vitalitas Sistem Elektronik					Sektor yang Terdampak Sistem Elektronik	Keterangan
	Dampak Operasional	Dampak terhadap Data dan/atau Informasi	Dampak Finansial	Dampak Umum	Dampak Saling Ketergantungan (*Interdependency*)		
(8)	(9)	(9)	(9)	(9)	(9)	(10)	(11)

Keterangan:

(1) Diisi dengan nomor urut.

(2) Diisi dengan salah satu Jenis Sistem Elektronik:
- *Core Banking System*
- *Internet banking* dan/atau *mobile banking*

(3) Diisi dengan Nama Sistem Elektronik yang diidentifikasi. Contoh: *Core Banking System Treasury*.

(4) Diisi dengan deskripsi singkat dan fungsi layanan yang dijalankan Sistem Elektronik.
Contoh: Sistem Elektronik memproses transaksi harian dan mengelola data nasabah.

(5) Diisi dengan daftar jenis data yang dikelola oleh Sistem Elektronik.
Contoh:
- *Data Nasabah*
- *Data Transaksi*
- *Data Keuangan*

(6) Diisi dengan informasi hubungan ketergantungan Sistem Elektronik dengan pihak ketiga (jika ada). Informasi terkait hubungan ketergantungan mencakup antara lain nama, deskripsi kerja sama, tanggal mulai kerja sama, dan informasi lain yang relevan. Contoh pihak ketiga yaitu PPJTI dalam penyelenggaraan *core banking system*.

(7) Diisi dengan ketersediaan rencana keberlangsungan layanan (dhi. BCP/BCM).
Contoh: Bank telah memiliki kebijakan, standar, dan prosedur terkait Rencana Pemulihan Bencana yang mencakup Sistem Elektronik X. Pengujian Rencana Pemulihan Bencana dilakukan minimum 1 (satu) tahun sekali dan terakhir kali dilakukan pada pertengahan tahun 2025.

(8) Diisi dengan kategori Sistem Elektronik, sesuai dengan Peraturan Badan Siber dan Sandi Negara mengenai identifikasi infrastruktur informasi vital (Strategis, Tinggi, atau Rendah).

Kategori Sistem Elektronik	Penjelasan
Strategis	Sistem Elektronik berdampak terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara
Tinggi	Sistem Elektronik berdampak pada kepentingan sektor dan/atau daerah tertentu
Rendah	Sistem Elektronik yang tidak termasuk pada kategori strategis dan tinggi

(9) Diisi dengan hasil pengukuran potensi skala dampak jika terjadi gangguan, kegagalan, kerusakan, dan/atau kehancuran pada Sistem Elektronik, sesuai dengan skala dampak sebagaimana diatur dalam lampiran Peraturan Badan Siber dan Sandi Negara mengenai identifikasi infrastruktur informasi vital (Serius, Signifikan, Terbatas, atau *Minor*), termasuk penjelasan atas penetapan skala dampak.

Contoh:

Berdasarkan hasil identifikasi, Sistem Elektronik memiliki dampak yang signifikan terhadap operasional karena kegagalan Sistem Elektronik mengakibatkan terhentinya layanan transaksi pada provinsi tertentu.

(10) Diisi dengan Sektor yang terdampak jika terjadi kegagalan atau gangguan, meliputi sektor:

a. administrasi pemerintahan;
b. energi dan sumber daya mineral;
c. transportasi;
d. keuangan;
e. kesehatan;
f. teknologi informasi dan komunikasi;
g. pangan;
h. pertahanan; dan
i. sektor lain yang ditetapkan oleh Presiden.

(11) Diisi dengan informasi tambahan yang relevan.

Format 3.3

LAPORAN HASIL AUDIT INTERN TEKNOLOGI INFORMASI

A. Informasi Pelapor

Nama Bank : .....
Alamat Kantor Pusat Bank : .....
Nomor Telepon : .....
Nama Narahubung : .....
Nomor Telepon Narahubung : .....
Kantor/Divisi/Bagian Pelapor: .....
Alamat Kantor/Divisi/Bagian Pelapor: .....
Tanggal Pelaporan: ..../..../..... (*dd/mm/yyyy*)

B. Laporan Hasil Audit TI *)

1. Lampirkan detail anggota tim pelaksana audit TI.
2. Jika audit TI dilaksanakan oleh pihak ekstern, lampirkan perjanjian kerja sama pelaksanaan audit antara Bank dengan pihak ekstern tersebut.**)
3. Berikan keterangan mengenai cakupan audit TI.
4. Berikan penjelasan kelemahan TI yang ditemukan, tindak lanjut penyelesaian, dan target waktu penyelesaian.

Keterangan:

*) Audit khusus TI dilaksanakan terhadap aspek-aspek yang terkait TI sesuai kebutuhan, prioritas, dan hasil analisis risiko TI Bank

**) Informasi mencakup jenis layanan, data penyedia jasa (nama perusahaan, alamat Pusat Data, alamat perusahaan, pemilik/grup pemilik mayoritas), tanggal dan jangka waktu perjanjian, narahubung di Bank yang menangani jasa penyelenggaraan TI tersebut dan informasi penting lain

Format 3.4.1

NOTIFIKASI AWAL INSIDEN TI (NONSIBER)

A. INFORMASI BANK

Nama Bank : .....(1)
Alamat Kantor Pusat Bank : **.....**(2)
Nomor Telepon : **.....**(3)
Nama Narahubung : .....(4)
Nomor Telepon Narahubung : **.....**(5)
Otoritas/Lembaga Penerima : **.....**(6)

B. INFORMASI UMUM INSIDEN TI (NONSIBER)

1. Tanggal dan Waktu Terjadinya Insiden TI: (7)
   ..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
2. Tanggal dan Waktu Insiden TI Diketahui: (8)
   ..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
3. Jenis Insiden TI : ....._(9)
4. Sistem Terdampak: .....(10)
5. Respons Awal Bank Pasca Insiden TI: ..... (11)
6. Penilaian Awal atas Dampak Insiden TI: .....(12)

Keterangan:
(1) Diisi dengan nama Bank.
(2) Diisi dengan Alamat kantor pusat Bank.
(3) Diisi dengan nomor telepon kantor pusat Bank.
(4) Diisi dengan nama Narahubung, yang bertanggung jawab untuk melaporkan insiden TI pada Bank.
(5) Diisi dengan Nomor Telepon dari Narahubung sebagaimana nomor (4).
(6) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima pelaporan notifikasi awal ini (jika ada).
(7) Diisi dalam hal Bank telah mengidentifikasi tanggal dan waktu terjadinya insiden TI.
(8) Diisi dengan tanggal dan waktu pada saat Bank mengetahui sedang terjadi Insiden TI.
(9) Diisi dengan informasi mengenai jenis insiden TI yang terjadi. Contoh: kebakaran pada DC/DRC Bank.
(10) Diisi dengan informasi mengenai nama sistem atau jaringan yang mengalami gangguan
(11) Diisi dengan informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden TI.
(12) Diisi dalam hal dampak insiden TI telah diidentifikasi oleh Bank (antara lain dampak kepada produk layanan Bank, operasional, finansial, dan/atau reputasi).

Format 3.4.2

LAPORAN INSIDEN TI (NONSIBER)

A. INFORMASI PELAPOR

Nama Bank : .....(1)
Alamat Kantor Pusat Bank : ..... (2)
Nomor Telepon : .....(3)
Nama Narahubung : .....(4)
Nomor Telepon Narahubung : .....(5)
Tanggal Penyampaian Notifikasi Awal: ..../..../..... (dd/mm/yyyy) (6)
Otoritas/Lembaga Penerima : ..... (7)

B. INFORMASI UMUM INSIDEN TI

1. Tanggal dan Waktu Terjadinya Insiden TI: (8)
..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
2. Tanggal dan Waktu Insiden TI Diketahui: (9)
..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
3. Jenis Insiden TI : .....(10)
4. Sistem Terdampak: .....(11)
5. Respons Awal Bank Pasca Insiden TI: ..... (12)

C. PENILAIAN ATAS DAMPAK INSIDEN TI BAGI BANK

1. Penilaian Dampak Insiden TI terhadap Ketersediaan dan Operasional Layanan Bank.....(13)
2. Penilaian Dampak Insiden TI terhadap Finansial Bank .....(14)
3. Penilaian Dampak Insiden TI terhadap Reputasi Bank .....(15)
4. Penilaian Dampak Insiden TI terhadap Aspek Hukum dan Kepatuhan Bank.....(16)
5. Penilaian Dampak Insiden TI terhadap Pihak Ketiga .....(17)
6. Penilaian Dampak Lain dari Insiden TI yang Dapat Diidentifikasi oleh Bank.....(18)

D. INFORMASI KRONOLOGIS INSIDEN TI(19)

E. ANALISIS PENYEBAB TERJADINYA INSIDEN(20)

F. ANALISIS FINAL

1. Kesimpulan(21)
2. Langkah Perbaikan(22)
3. Target Waktu Penyelesaian Insiden TI: ..... (*dd/mm/yyyy*)(23)

Keterangan:
(1) Diisi dengan nama Bank.
(2) Diisi dengan Alamat kantor pusat Bank.
(3) Diisi dengan nomor telepon kantor pusat Bank.
(4) Diisi dengan Nama Narahubung, yang bertanggung jawab untuk melaporkan insiden TI pada Bank.
(5) Diisi dengan Nomor Telepon dari Narahubung sebagaimana dimaksud pada nomor (4).
(6) Diisi dengan tanggal penyampaian notifikasi awal Insiden TI.
(7) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima pelaporan notifikasi awal ini (jika ada).
(8) Diisi dalam hal Bank telah mengidentifikasi tanggal dan waktu terjadinya insiden TI
(9) Diisi dengan tanggal dan waktu pada saat Bank mengetahui sedang terjadi Insiden TI
(10) Diisi dengan informasi mengenai jenis insiden TI yang terjadi. Contoh: kebakaran pada DC/DRC Bank.
(11) Diisi dengan informasi mengenai nama sistem atau jaringan yang mengalami gangguan.
(12) Diisi dengan informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden TI.
(13) Diisi dalam hal terdapat dampak terhadap bisnis Bank, termasuk dalam kaitannya dengan ketersediaan dan operasional layanan Bank. Informasi memuat paling sedikit:
    a. jenis layanan dan/atau nama produk yang terdampak (contoh: layanan *treasury*, *trade finance*, *cash management*, dan layanan perbankan digital); dan
    b. penjelasan mengenai dampak yang terjadi (jika layanan dan/atau produk yang terdampak lebih dari 1 (satu), maka penjelasan diberikan untuk seluruh layanan dan produk yang terdampak).
(14) Diisi dalam hal terdapat dampak finansial dari insiden siber, Informasi memuat paling sedikit:
    a. hal yang terdampak (contoh: nilai atau volume transaksi, penarikan dana, dan likuiditas Bank); dan
    b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) hal maka penjelasan diberikan untuk seluruh hal yang terdampak).
(15) Diisi dalam hal terdapat dampak terhadap reputasi Bank dari insiden siber (contoh: insiden TI dipublikasikan oleh media).
(16) Diisi dalam hal terdapat dampak terhadap aspek hukum dan kepatuhan (contoh: pelanggaran ketentuan peraturan perundang-undangan dan adanya tuntutan hukum dari pihak terkait).
(17) Diisi dalam hal terdapat dampak terhadap pihak ketiga dari Bank. Informasi paling sedikit memuat:
    a. kategori pihak ketiga (contoh: nasabah, pihak penyedia jasa, dan mitra kerja sama layanan); dan
    b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) kategori mitra maka penjelasan diberikan untuk seluruh mitra terdampak).
(18) Diisi dengan hal lain yang terdampak Insiden TI.
(19) Diisi dengan penjelasan kronologis terjadinya insiden TI, yang memuat:
    a. Durasi terjadinya insiden TI.
    b. Langkah eskalasi insiden TI yang dilakukan.
    c. Langkah penanggulangan insiden TI yang dilakukan.
    d. Langkah pemulihan insiden TI yang dilakukan.
    e. Keterlibatan pihak ketiga dalam penanggulangan dan pemulihan insiden TI.
    f. Pihak yang menerima informasi terkait insiden TI (pemangku kepentingan, contoh: otoritas, mitra layanan, dan nasabah).
    g. Informasi pendukung lain.
(20) Diisi dengan hasil identifikasi Bank atas penyebab terjadinya insiden TI, termasuk terdapat unsur atau tidak yang menyebabkan terjadinya insiden TI.
(21) Diisi dengan informasi yang dapat menyimpulkan penyebab, kronologi dan dampak atas insiden TI yang terjadi.

(22) Diisi dengan informasi mengenai langkah yang dilakukan Bank untuk mencegah insiden TI serupa terjadi di masa depan.
(23) Diisi dalam hal insiden TI belum sepenuhnya diselesaikan pada saat menyampaikan laporan kepada Otoritas Jasa Keuangan.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN IV
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2026
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

FORMAT PERMOHONAN IZIN DAN LAPORAN REALISASI

DAFTAR ISI

4.1 Format Formulir dan Dokumen Permohonan Izin Penempatan Sistem Elektronik Pada Pusat Data dan/atau Pusat Pemulihan Bencana di Luar Wilayah Indonesia

PERMOHONAN IZIN PENEMPATAN SISTEM ELEKTRONIK PADA PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA

1. Informasi Pemohon

   Nama Bank : .....

   Alamat Kantor Pusat Bank : .....

   Nomor Telepon : .....

   Nama Narahubung : .....

   Nomor Telepon Narahubung : .....

   Tanggal Permohonan : .../.../.... (dd/mm/yyyy)

2. Informasi dan Dokumen terkait Pusat Data/Pusat Pemulihan Bencana
   a) Lokasi Pusat Data : .....
   b) Lokasi Pusat Pemulihan Bencana : .....
      .....
   c) Nama Penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana : .....
      .....
      .....
   d) Alamat penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana : .....
      .....
      .....
   e) Ringkasan analisis Bank atas hasil audit TI oleh pihak independen terhadap sistem pengamanan pada Pusat Data/Pusat Pemulihan Bencana.*)

3. Informasi dan Dokumen terkait Sistem Elektronik
   a) Nama Sistem Elektronik : .....
   b) Fungsi Sistem Elektronik : .....
   c) Ringkasan hasil analisis kebutuhan yang telah dilakukan Bank dalam rencana penggunaan Sistem Elektronik.
   d) Ringkasan hasil uji tuntas (*due diligence*) terhadap PPJTI, meliputi analisis kinerja, reputasi, dan kelangsungan penyediaan layanan. Serta melampirkan ringkasan:
      1) analisis Bank atas hasil audit TI yang dilakukan oleh pihak independen terhadap pengembangan sistem aplikasi yang ditawarkan;
      2) analisis risiko Bank mengenai penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia, antara lain risiko operasional, hukum, dan reputasi serta analisis *country risk*;
      3) analisis atas pengendalian pengamanan oleh PPJTI untuk memastikan terpenuhinya kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan keaslian (*authentication*) terhadap Sistem Elektronik.
   e) Konsep perjanjian antara Bank dengan PPJTI.
   f) Ringkasan analisis biaya dan manfaat yang terukur, yang menunjukkan manfaat bagi Bank lebih besar dari biaya yang dibebankan oleh PPJTI kepada Bank.

g) Gambar arsitektur TI terkait Sistem Elektronik, yang menggambarkan kondisi saat ini dan setelah implementasi.

4. Ringkasan analisis Bank mengenai kecukupan Rencana Pemulihan Bencana milik PPJTI.
5. Surat pernyataan dari Bank mengenai kesediaan Bank memberikan akses kepada auditor intern, ekstern maupun Otoritas Jasa Keuangan untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.
6. Dalam hal Bank merupakan kantor cabang dari bank yang berkedudukan di luar negeri atau Bank yang dimiliki lembaga keuangan asing, Bank melampirkan:
   a) Surat pernyataan dari otoritas pengawas di bidang keuangan di luar negeri bahwa PPJTI merupakan cakupan pengawasannya;
   b) Surat pernyataan tidak keberatan dari otoritas pengawas di bidang keuangan jika Otoritas Jasa Keuangan hendak melakukan pemeriksaan penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana tersebut;
   c) Surat pernyataan bahwa Bank menyampaikan secara berkala hasil penilaian yang dilakukan kantor bank di luar wilayah Indonesia atas penerapan manajemen risiko pada PPJTI; dan
   d) Hasil penilaian yang dilakukan kantor bank di luar wilayah Indonesia atas penerapan manajemen risiko pada PPJTI.
7. Rencana Bank mengenai peningkatan kemampuan SDM yang berkaitan dengan penyelenggaraan Sistem Elektronik yang ditempatkan pada Pusat Data/Pusat Pemulihan Data di luar wilayah Indonesia.

Keterangan:

*) Hanya disampaikan dalam hal Bank pertama kali menempatkan Sistem Elektronik pada DC/DRC tersebut.

4.2 Format Formulir dan Dokumen Laporan Realisasi Penempatan Sistem Elektronik Pada Pusat Data dan/atau Pusat Pemulihan Bencana di Luar Wilayah Indonesia

LAPORAN REALISASI PENEMPATAN SISTEM ELEKTRONIK PADA PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA

1. Informasi Pelapor
   Nama Bank : .....
   Alamat Kantor Pusat Bank : .....
   Nomor Telepon : .....
   Nama Narahubung : .....
   Nomor Telepon Narahubung : .....
   Tanggal Realisasi : .../.../..... (*dd/mm/yyyy*)
2. Informasi dan Dokumen terkait Pusat Data/Pusat Pemulihan Bencana
   a) Lokasi Pusat Data : .....
   b) Lokasi Pusat Pemulihan Bencana : .....
   c) Nama Penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana : .....
   d) Alamat penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana : .....
3. Informasi dan Dokumen terkait Sistem Elektronik
   a) Nama Sistem Elektronik : .....
   b) Fungsi Sistem Elektronik : .....
   c) Hasil analisis terkini atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dalam penyelenggaraan yang diserahkan kepada PPJTI.
   d) Salinan perjanjian antara Bank dan penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana.
   e) Uraian analisis risiko terkini Bank terhadap penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana oleh PPJTI di luar wilayah Indonesia tersebut antara lain risiko operasional, hukum, dan reputasi, serta analisis *country risk*.
4. Hasil kajian pascaimplementasi (*post-implementation review*/PIR) atas penggunaan Pusat Data PPJTI yang antara lain mencakup hasil kaji ulang mengenai:
   a) Kinerja sistem (*system performance review*);
   b) Kesesuaian dengan kebutuhan pengguna (*user requirement*);
   c) Masalah yang terjadi beserta solusi, eskalasi, atau langkah penyelesaian yang dilakukan; dan
   d) Efektivitas pengamanan yang ditetapkan.
5. Hasil pengujian atas penggunaan Pusat Pemulihan Bencana yang diselenggarakan PPJTI tersebut.
6. Berita acara pengalihan Pusat Data dan/atau Pusat Pemulihan Bencana.
7. Gambar arsitektur TI terkini setelah penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana diserahkan kepada PPJTI.

4.3 Format Formulir dan Dokumen Permohonan Izin Pemrosesan Transaksi Berbasis TI oleh PPJTI di Luar Wilayah Indonesia

PERMOHONAN IZIN PEMROSESAN TRANSAKSI BERBASIS TEKNOLOGI INFORMASI OLEH PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI DI LUAR WILAYAH INDONESIA

1. Informasi Pemohon
   Nama Bank : .....
   Alamat Kantor Pusat Bank : .....
   Nomor Telepon : .....
   Nama Narahubung : .....
   Nomor Telepon Narahubung : .....
   Tanggal Permohonanan : .../.../..... (*dd/mm/yyyy*)
2. Uraian atau penjelasan dan *flow chart* dari standar prosedur pelaksanaan (*Standard Operating System*) dari produk dan aktivitas yang penyelenggaraannya akan diserahkan kepada PPJTI.
3. Informasi dan Dokumen terkait Pusat Data/Pusat Pemulihan Bencana
   a) Lokasi Pusat Data : .....
   b) Lokasi Pusat Pemulihan Bencana : .....
4. Informasi dan Dokumen terkait Pemrosesan Transaksi
   a) Lokasi Pemrosesan Transaksi Berbasis TI : .....
   b) Nama Penyelenggara Pemrosesan Transaksi Berbasis TI : .....
   c) Alamat Penyelenggara Pemrosesan Transaksi Berbasis TI : .....
   d) Ringkasan hasil analisis kebutuhan yang telah dilakukan Bank dalam rencana penggunaan Sistem Elektronik.
   e) Ringkasan hasil uji tuntas (*due diligence*) terhadap PPJTI, meliputi analisis kinerja, reputasi, dan kelangsungan penyediaan layanan. Serta melampirkan ringkasan:
      1) analisis Bank atas hasil audit TI yang dilakukan oleh pihak independen terhadap pengembangan sistem aplikasi yang akan digunakan untuk memproses transaksi oleh PPJTI.
      2) analisis risiko Bank atas rencana menyerahkan penyelenggaraan pemrosesan transaksi berbasis TI kepada PPJTI antara lain risiko operasional, hukum, dan reputasi, serta analisis *country risk*; dan
      3) analisis atas pengendalian pengamanan oleh PPJTI untuk memastikan terpenuhinya kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan keaslian (*authentication*).
   f) Konsep perjanjian antara Bank dengan PPJTI
   g) Ringkasan analisis biaya dan manfaat yang terukur, yang antara lain mencakup:
      1) manfaat bagi Bank lebih besar dari biaya yang dibebankan oleh PPJTI kepada Bank; dan
      2) penilaian kecukupan dan kesesuaian sistem aplikasi yang akan digunakan dengan kebutuhan Bank.
   h) Gambar alur proses pelaporan dan informasi saat ini dan setelah implementasi.

5. Ringkasan analisis Bank mengenai kecukupan Rencana Pemulihan Bencana milik PPJTI.
6. Surat pernyataan dari Bank mengenai kesediaan Bank memberikan akses kepada auditor intern, ekstern maupun Otoritas Jasa Keuangan untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.
7. Rencana Bank mengenai penerapan aspek perlindungan kepada nasabah atas produk yang pemrosesannya diserahkan kepada PPJTI.
8. Rencana Bank mengenai peningkatan peran Bank bagi perkembangan perekonomian Indonesia melalui rencana bisnis.

4.4 Format Formulir dan Dokumen Laporan Realisasi Pemrosesan Transaksi Berbasis TI oleh PPJTI di Luar Wilayah Indonesia

LAPORAN REALISASI PEMROSESAN TRANSAKSI BERBASIS TEKNOLOGI INFORMASI OLEH PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI DI LUAR WILAYAH INDONESIA

1. Informasi Pelapor
   Nama Bank : .....
   Alamat Kantor Pusat Bank : .....
   Nomor Telepon : .....
   Nama Narahubung : .....
   Nomor Telepon Narahubung : .....
   Tanggal Realisasi : .../.../..... (*dd/mm/yyyy*)
2. Informasi dan Dokumen terkait Pusat Data/Pusat Pemulihan Bencana
   a) Lokasi Pusat Data : .....
   b) Lokasi Pusat Pemulihan Bencana : .....
3. Informasi dan Dokumen terkait Pemrosesan Transaksi
   a) Lokasi Pemrosesan Transaksi Berbasis TI : .....
      .....
   b) Nama Penyelenggara Pemrosesan Transaksi Berbasis TI : .....
      .....
   c) Alamat Penyelenggara Pemrosesan Transaksi Berbasis TI : .....
      .....
   d) Hasil analisis terkini atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dalam penyelenggaraan pemrosesan transaksi berbasis TI yang diserahkan kepada PPJTI.
   e) Salinan perjanjian antara Bank dan pihak penyedia jasa penyelenggaraan pemrosesan transaksi berbasis TI di luar wilayah Indonesia.
   f) Uraian atau penjelasan dan *flow chart* dari standar prosedur pelaksanaan (*Standard Operating Procedure*) produk dan aktivitas Bank yang penyelenggaraannya diserahkan kepada PPJTI.
4. Hasil kajian pascaimplementasi (*post-implementation review*/PIR) atas penggunaan PPJTI dalam menyelenggarakan pemrosesan transaksi berbasis TI yang antara lain mencakup hasil kaji ulang mengenai:
   a) Kinerja sistem (*system performance review*);
   b) Kesesuaian dengan kebutuhan pengguna (*user requirement*);
   c) Masalah yang terjadi beserta solusi, eskalasi, atau langkah penyelesaian yang dilakukan; dan
   d) Efektivitas pengamanan yang ditetapkan.
5. Hasil pengujian atas penggunaan penyelenggaraan pemrosesan transaksi berbasis TI di luar wilayah Indonesia.
6. Berita acara pengalihan penyelenggaraan pemrosesan transaksi berbasis TI.
7. Gambar alur proses pelaporan dan informasi terkini setelah penyelenggaraan pemrosesan transaksi berbasis TI diserahkan kepada PPJTI.

4.5 Format Formulir dan Dokumen Permohonan Izin Penyediaan Jasa TI oleh Bank

PERMOHONAN IZIN
PENYEDIAAN JASA TEKNOLOGI INFORMASI OLEH BANK

A. Informasi Pemohon

Nama Bank : .....

Alamat Kantor Pusat Bank : .....

Nomor Telepon : .....

Nama Narahubung : .....

Nomor Telepon Narahubung : .....

Tanggal Permohonan : .../.../..... (*dd/mm/yyyy*)

B. Informasi dan Dokumen terkait Penyediaan Jasa TI oleh Bank

1. Jenis jasa TI yang akan disediakan oleh Bank:

No.	Jenis Jasa TI	Ya/Tidak*)
1	Pusat Data	
2	Pusat Pemulihan Bencana	
3	Jaringan Komunikasi	
4	Layanan Aplikasi	
5	Lainnya: .... (sebutkan)	

2. Pihak penerima jasa TI
   a. Nama perusahaan : .....
   b. Alamat : .....
   c. Deskripsi singkat usaha : .....
   d. Hubungan dengan Bank : .....
3. Informasi umum terkait jasa TI yang akan disediakan Bank
   a. Lokasi penyelenggaraan
      Pusat Data : .....
      Pusat Pemulihan Bencana : .....
   b. Daftar jasa TI berupa layanan aplikasi yang disediakan oleh Bank

No.	Jenis Layanan Aplikasi	Nama Layanan Aplikasi	Keterangan dan Tujuan Layanan Aplikasi
1	Contoh: Layanan Digital	*Mobile* IM	...
2	Contoh: Sistem Remunerasi Pegawai	SiRemun	...
...	...	...	...
...	...	...	...

4. Jika Bank menyediakan jasa TI berupa Pusat Data dan/atau Pusat Pemulihan Bencana maka lampirkan analisis kecukupan kapasitas Pusat Data dan/atau Pusat Pemulihan Bencana Bank (contoh: ruangan dan jaringan) untuk kebutuhan bisnis Bank pada masa mendatang dengan memperhitungkan kapasitas Pusat Data dan/atau Pusat Pemulihan Bencana yang disediakan oleh Bank kepada pihak lain.
5. Analisis biaya dan manfaat penyediaan jasa TI yang dapat memperlihatkan manfaat bagi Bank melampaui biaya atas penyediaan jasa TI.
6. Analisis risiko terhadap penyediaan jasa TI yang memuat paling sedikit aspek operasional, reputasi, hukum, kepatuhan, dan strategis serta mitigasi yang harus dilakukan Bank untuk memastikan terpenuhinya

kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan keaslian (*authenticity*) terhadap penyediaan jasa TI

7. Konsep perjanjian antara Bank dengan pengguna jasa TI.

Keterangan:
*) Pilih salah satu sesuai dengan rencana penyediaan jasa TI.

4.6 Format Formulir dan Dokumen Laporan Realisasi Penyediaan Jasa TI oleh Bank

LAPORAN REALISASI PENYEDIAAN JASA TI OLEH BANK

A. Informasi Pelapor

Nama Bank : .....
Alamat Kantor Pusat Bank : .....
Nomor Telepon : .....
Nama Narahubung : .....
Nomor Telepon Narahubung : .....
Tanggal Pelaporan : .../.../..... (*dd/mm/yyyy*)

B. Laporan Realisasi

1. Jenis jasa TI yang disediakan oleh Bank
   a. Pusat Data

Tanggal Realisasi	(*dd/mm/yyyy*)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerja sama	(*dd/mm/yyyy* s.d. *dd/mm/yyyy*)

   b. Pusat Pemulihan Bencana

Tanggal Realisasi	(*dd/mm/yyyy*)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerja sama	(*dd/mm/yyyy* s.d. *dd/mm/yyyy*)

   c. Jaringan Komunikasi

Tanggal Realisasi	(*dd/mm/yyyy*)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerja sama	(*dd/mm/yyyy* s.d. *dd/mm/yyyy*)

   d. Layanan Aplikasi

Tanggal Realisasi	(*dd/mm/yyyy*)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerja sama	(*dd/mm/yyyy* s.d. *dd/mm/yyyy*)

   e. Penyediaan Jasa TI Lainnya

Tanggal Realisasi	(*dd/mm/yyyy*)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerja sama	(*dd/mm/yyyy* s.d. *dd/mm/yyyy*)

2. Pihak pengguna jasa TI
   a. Nama perusahaan : .....
   b. Alamat : .....
   c. Deskripsi singkat usaha : .....
   d. Hubungan dengan Bank : .....
3. Informasi umum terkait jasa TI yang disediakan oleh Bank
   a. Lokasi penyelenggaraan
      Pusat Data : .....
      Pusat Pemulihan Bencana : .....

b. Daftar layanan jasa aplikasi yang disediakan oleh Bank:

No.	Jenis Layanan Aplikasi	Nama Layanan Aplikasi	Keterangan dan Tujuan Layanan Aplikasi
1	Contoh: Layanan Digital	*Mobile* IM	…
2	Contoh: Sistem Remunerasi Pegawai	SiRemun	…
3	…	…	…
4	…	…	…

4. Perjanjian antara Bank dengan lembaga jasa keuangan pengguna yang sudah merealisasikan penggunaan layanan jasa TI.
5. Berita acara atas penyediaan layanan jasa TI yang disediakan oleh Bank sudah digunakan oleh lembaga jasa keuangan.
6. Hasil kajian pascaimplementasi (*post-implementation review*/PIR) atas penyediaan jasa TI oleh Bank, yang antara lain mencakup hasil kaji ulang mengenai:
   a. Kinerja sistem (*system performance review*);
   b. Kesesuaian dengan kebutuhan pengguna (*user requirement*);
   c. Masalah yang terjadi beserta solusi, eskalasi, atau langkah penyelesaian yang dilakukan;
   d. Efektivitas pengamanan yang ditetapkan; dan
   e. Pemenuhan *Service Level Agreement*/SLA.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi