Yth.

1. Direksi Bank Umum Konvensional; dan
2. Direksi Bank Umum Syariah,

di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 21 /SEOJK.03/2017

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM

PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 267, Tambahan Lembaran Negara Republik Indonesia Nomor 5963) selanjutnya disingkat POJK MRTI, perlu untuk mengatur ketentuan pelaksanaan mengenai penerapan manajemen risiko dalam penggunaan Teknologi Informasi oleh bank umum dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Pedoman penerapan manajemen risiko dalam penggunaan Teknologi Informasi oleh bank umum merupakan acuan standar penerapan manajemen risiko dalam penggunaan Teknologi Informasi oleh Bank.
2. Bank yang telah memiliki kebijakan, standar, dan prosedur dalam penggunaan Teknologi Informasi dan/atau pedoman manajemen risiko penggunaan Teknologi Informasi sebelum berlakunya Surat Edaran Otoritas Jasa Keuangan ini, menyesuaikan dan menyempurnakan dengan berpedoman pada Lampiran I yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

II. PEDOMAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI

1. Dalam rangka menerapkan manajemen risiko penggunaan Teknologi Informasi untuk mendukung kelangsungan bisnis Bank terutama pelayanan kepada nasabah, Bank wajib memiliki kebijakan, standar, dan prosedur penggunaan Teknologi Informasi serta wajib menerapkan kebijakan, standar, dan prosedur penggunaan Teknologi Informasi secara konsisten dan berkesinambungan sebagaimana telah diatur dalam Pasal 8 ayat (1) POJK MRTI.
2. Kebijakan, standar, dan prosedur penggunaan Teknologi Informasi serta pedoman manajemen risiko penggunaan Teknologi Informasi mengacu pada Lampiran I yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini dan mengacu pada Surat Edaran Otoritas Jasa Keuangan Nomor 34/SEOJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum.
3. Kebijakan, standar, dan prosedur penggunaan Teknologi Informasi paling sedikit meliputi aspek:
   a. manajemen;
   b. pengembangan dan pengadaan;
   c. operasional Teknologi Informasi;
   d. jaringan komunikasi;
   e. pengamanan informasi;
   f. Rencana Pemulihan Bencana;
   g. Layanan Perbankan Elektronik;
   h. penggunaan pihak penyedia jasa Teknologi Informasi; dan
   i. penyediaan jasa Teknologi Informasi oleh Bank.
4. Aspek kebijakan, standar, dan prosedur penggunaan Teknologi Informasi sebagaimana dimaksud pada angka 3 harus diterapkan oleh Bank untuk memitigasi risiko yang berhubungan dengan penyelenggaraan Teknologi Informasi.
5. Bank dengan ukuran dan kompleksitas usaha besar dapat menggunakan parameter tambahan dari yang diatur dalam pedoman sebagaimana dimaksud dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

III. PELAPORAN

1. Dalam menerapkan manajemen risiko penggunaan Teknologi Informasi, Bank menyampaikan laporan-laporan sebagai berikut:
   a. Laporan kondisi terkini penggunaan Teknologi Informasi dengan ketentuan sebagai berikut:
      1) Laporan menggunakan format sebagaimana dimaksud pada Lampiran 2.1. yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
      2) Laporan disampaikan paling lambat 1 (satu) bulan sejak akhir tahun pelaporan.
   b. Laporan rencana pengembangan Teknologi Informasi yang akan diimplementasikan 1 (satu) tahun ke depan dengan ketentuan sebagai berikut:
      1) Laporan menggunakan format sebagaimana dimaksud pada Lampiran 2.2. yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
      2) Laporan disampaikan paling lambat pada tanggal 31 Oktober tahun sebelumnya.
      3) Laporan dapat diubah 1 (satu) kali dan disampaikan paling lambat pada tanggal 30 Juni tahun berjalan.
      4) Pengajuan perubahan laporan rencana pengembangan Teknologi Informasi dapat dilakukan selain dalam jangka waktu sebagaimana dimaksud pada angka 3) sepanjang memenuhi pertimbangan tertentu dan mendapatkan persetujuan dari Otoritas Jasa Keuangan.
   c. Laporan realisasi:
      1) kegiatan sebagai penyedia jasa Teknologi Informasi;
      2) penerbitan produk Layanan Perbankan Elektronik;
      3) penyelenggaraan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia; dan
      4) penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi kepada pihak penyedia jasa di luar wilayah Indonesia;

      dengan ketentuan sebagai berikut:
      i. Laporan menggunakan format sebagaimana dimaksud pada Lampiran 2.4. yang merupakan bagian tidak terpisahkan

dari Surat Edaran Otoritas Jasa Keuangan ini.

ii. Laporan disampaikan paling lambat 3 (tiga) bulan setelah implementasi.

d. Laporan insidentil mengenai kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraaan Teknologi Informasi yang dapat dan/atau telah mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank, dengan ketentuan sebagai berikut:

1) Laporan menggunakan format sebagaimana dimaksud pada Lampiran 2.5. yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

2) Laporan disampaikan dengan segera kepada Otoritas Jasa Keuangan melalui surat elektronik (*electronic mail*) atau telepon yang diikuti dengan laporan tertulis paling lama 7 (tujuh) hari kerja setelah kejadian kritis dan/atau penyalahgunaan atau kejahatan diketahui.

e. Laporan hasil audit Teknologi Informasi dengan ketentuan sebagai berikut:

1) Laporan menggunakan format sebagaimana dimaksud pada Lampiran 2.6. yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

2) Laporan disampaikan paling lambat 2 (dua) bulan setelah audit Teknologi Informasi selesai dilakukan.

2. Bank yang menyerahkan penyelenggaraan Teknologi Informasi kepada penyedia jasa Teknologi Informasi tetap menyampaikan laporan sebagaimana dimaksud pada angka 1 kepada Otoritas Jasa Keuangan.

IV. PERMOHONAN PERSETUJUAN

1. Bank yang memiliki rencana kegiatan sebagai penyedia jasa Teknologi Informasi dan/atau menerbitkan produk Layanan Perbankan Elektronik, harus mengajukan permohonan persetujuan kepada Otoritas Jasa Keuangan paling lambat 2 (dua) bulan sebelum implementasi.

2. Bank yang menyelenggarakan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia serta Bank yang menyerahkan penyelenggaraan

Pemrosesan Transaksi Berbasis Teknologi Informasi kepada pihak penyedia jasa di luar wilayah Indonesia, harus mengajukan permohonan persetujuan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan sebelum rencana implementasi.

Permohonan persetujuan pada angka 1 dan 2 disertai dengan dokumen sebagaimana tercantum dalam Lampiran 2.3 yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

V. PENUTUP

Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 6 Juni 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

ttd

NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana

LAMPIRAN I

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 21 /SEOJK.03/2017

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM

PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

PEDOMAN PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DAFTAR ISI

KATA PENGANTAR

Teknologi Informasi (TI) saat ini memainkan peran yang sangat penting dalam kegiatan perbankan. Dari yang semula hanya berperan sebagai pendukung kegiatan operasional Bank, sekarang menjadi penentu arah kegiatan operasional Bank. Hal ini antara lain tercermin dari semakin banyaknya produk dan aktivitas perbankan yang memanfaatkan penggunaan TI, yang diharapkan dapat meningkatkan layanan kepada nasabah ditengah semakin ketatnya kompetisi antar Bank. Keandalan Bank mengelola TI juga menentukan keberhasilan Bank dalam menghasilkan suatu informasi yang lengkap, akurat, terkini, tepat waktu, dan relevan. Dengan demikian, informasi yang dihasilkan dapat mendukung proses pengambilan keputusan dan operasional bisnis Bank.

Penggunaan TI selain meningkatkan kecepatan dan keakuratan transaksi serta pelayanan kepada nasabah juga meningkatkan risiko seperti risiko operasional, risiko reputasi, risiko hukum, risiko kepatuhan, dan risiko stratejik. Untuk itu diharapkan Bank memiliki manajemen risiko yang terpadu untuk melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko. Namun demikian, mengingat terdapat perbedaan kondisi pasar, struktur, ukuran, dan kompleksitas usaha Bank maka tidak terdapat satu sistem manajemen risiko yang universal untuk seluruh Bank sehingga setiap Bank harus membangun sistem manajemen risiko yang sesuai dengan fungsi dan organisasi manajemen risiko pada Bank.

Pedoman ini merupakan pokok-pokok penerapan manajemen risiko dalam penggunaan TI yang harus diterapkan oleh Bank untuk memitigasi risiko yang berhubungan dengan penyelenggaraan TI. Bank dengan ukuran dan kompleksitas usaha besar hendaknya dapat menggunakan parameter tambahan dari yang diatur dalam pedoman. Bank juga diharapkan menerapkan kerangka manajemen risiko ini dengan memperhatikan peraturan perundang-undangan, standar yang ditetapkan, dan *best practices* untuk memastikan bahwa manajemen risiko yang memadai telah diterapkan.

BAB I MANAJEMEN

1.1. Pendahuluan

TI merupakan bagian yang penting dalam mendukung bisnis Bank baik untuk melakukan proses transaksi dengan nasabah maupun untuk menunjang kegiatan internal Bank. Dalam rangka meminimalisasi terjadinya risiko yang terkait dengan penggunaan TI dan untuk melindungi kepentingan Bank dan nasabah, Bank perlu menerapkan tata kelola TI (*Information Technology governance*). Keberhasilan penerapan tata kelola TI sangat tergantung pada komitmen dari Direksi, Dewan Komisaris, dan seluruh unit kerja di Bank, baik penyelenggara maupun pengguna TI. Penerapan tata kelola TI dilakukan melalui penyelarasan Rencana Strategis TI dengan strategi bisnis Bank, optimalisasi pengelolaan sumber daya, pemanfaatan TI, pengukuran kinerja, dan penerapan manajemen risiko yang efektif.

Perwujudan dari komitmen Direksi dan Dewan Komisaris dalam bentuk pengawasan aktif Direksi dan Dewan Komisaris terhadap manajemen TI sebagaimana telah diatur dalam Pasal 2 POJK MRTI. Sehubungan dengan hal itu, diperlukan kebijakan yang memuat peran dan tanggung jawab Direksi, Dewan Komisaris, dan pejabat tertinggi TI dalam memastikan diterapkannya manajemen risiko TI secara efektif.

1.2. Peran dan Tanggung Jawab Manajemen

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

1.2.1. Direksi

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

a. memastikan tersedianya sumber daya manusia (SDM) yang cukup dan kompeten sesuai dengan kebutuhan;
b. memastikan terdapat upaya peningkatan kompetensi SDM terkait penyelenggaraan TI diantaranya 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; dan
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.

1.2.2. Dewan Komisaris

Selain wewenang dan tanggung jawab bagi Dewan Komisaris sebagaimana diatur dalam Pasal 6 POJK MRTI, 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; dan
d. melakukan evaluasi terhadap pengelolaan pengamanan yang andal dan efektif atas TI guna menjamin ketersediaan, kerahasiaan, dan keakuratan informasi.

1.2.3. Komite Pengarah TI

Berdasarkan Pasal 7 POJK MRTI, Bank wajib memiliki komite pengarah TI (*Information Technology steering committee*). Hal ini berlaku juga untuk kantor cabang dari bank yang berkedudukan di luar negeri. Fungsi komite pengarah TI dapat dilaksanakan oleh fungsi sejenis yang berada di kantor pusat atau kantor regional bank.

Dalam melaksanakan tugasnya, 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 perlu melakukan pertemuan secara berkala

untuk membicarakan hal-hal yang terkait dengan strategi TI, yang didokumentasikan dalam bentuk risalah rapat.

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

a. Rencana Strategis TI yang sejalan dengan rencana strategis kegiatan usaha Bank. Dalam memberikan rekomendasi, komite pengarah TI harus memperhatikan faktor efisiensi, efektivitas, dan hal-hal lain, yaitu:
   1) peta jalan (*road-map*) untuk mencapai kebutuhan TI yang mendukung strategi bisnis Bank. Peta jalan (*road-map*) 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 Rencana Strategis TI diterapkan; dan
   4) kendala yang mungkin timbul dalam penerapan Rencana Strategis TI;
b. perumusan kebijakan, standar, dan prosedur TI yang utama, misalnya kebijakan TI yang utama yaitu kebijakan pengamanan TI dan manajemen risiko terkait penggunaan TI di Bank;
c. kesesuaian antara proyek TI yang disetujui dengan Rencana Strategis TI. Komite pengarah TI juga menetapkan status prioritas proyek TI yang bersifat kritikal yang berdampak signifikan terhadap kegiatan operasional Bank, misalnya pergantian *core banking application*, *server production,* dan topologi jaringan;
d. kesesuaian antara pelaksanaan proyek TI dengan rencana proyek yang disepakati (*project charter*). Komite pengarah TI harus melengkapi rekomendasi dengan hasil analisis dari proyek TI yang utama sehingga memungkinkan Direksi mengambil keputusan secara efisien;
e. kesesuaian antara TI dengan kebutuhan sistem informasi manajemen serta kebutuhan kegiatan usaha Bank;
f. efektivitas langkah-langkah dalam meminimalisasi risiko atas investasi Bank pada sektor TI agar investasi Bank pada sektor TI

memberikan kontribusi terhadap pencapaian tujuan bisnis Bank;

g. pemantauan atas kinerja TI dan upaya peningkatan kinerja TI, misalnya pendeteksian keusangan infrastruktur TI dan pengukuran efektivitas dan efisiensi penerapan kebijakan pengamanan TI;

h. upaya penyelesaian berbagai masalah terkait TI yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara TI secara efektif, efisien, dan tepat waktu; dan

i. kecukupan dan alokasi sumber daya 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.

1.2.4. Pejabat Tertinggi yang Memimpin Satuan Kerja TI

Dalam Pasal 7 POJK MRTI, diatur bahwa salah satu anggota komite pengarah TI adalah pejabat tertinggi yang memimpin satuan kerja TI. Dengan memperhatikan kompleksitas usaha Bank, posisi tersebut dapat dijabat oleh direktur TI atau pimpinan satuan kerja TI.

Wewenang dan tanggung jawab utama dari pejabat tertinggi yang memimpin satuan kerja TI paling sedikit mencakup:

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 perlindungan 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 pihak penyedia jasa TI;
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 yang secara langsung membawahi TI adalah direktur. Apabila pejabat tertinggi bukan seorang direktur maka pengawasan dapat dilakukan oleh direktur yang membawahkan kedua bidang tersebut;
m. bertanggung jawab terhadap penyusunan dan implementasi arsitektur TI serta rencana strategis lain yang mempengaruhi modal Bank secara signifikan, dalam hal pejabat tertinggi adalah direktur TI. Direktur TI harus memastikan struktur organisasi manajemen proyek dari seluruh proyek terkait TI digunakan secara maksimal. Apabila tidak ada pejabat yang mengisi posisi direktur TI maka hal tersebut menjadi tanggung jawab direktur yang membawahkan satuan kerja TI, misalnya satuan kerja TI tersebut berada di bawah direktur operasional maka fungsi tersebut menjadi tanggung jawab direktur operasional; dan
n. memastikan bahwa kontrak tertulis antara Bank dengan pihak penyedia jasa TI mencakup hal-hal yang diatur bagi penggunaan

pihak penyedia jasa TI.

1.3. Struktur Organisasi Satuan Kerja TI

Bank perlu memiliki struktur organisasi yang sesuai dengan kebutuhan penyelenggaraan dan penggunaan TI, paling sedikit memperhatikan:

a. struktur organisasi secara spesifik menggambarkan garis kewenangan, pelaporan, dan tanggung jawab untuk setiap fungsi TI yang dimiliki, termasuk pihak yang ditunjuk sebagai orang pengganti;

b. struktur organisasi yang tidak membuka peluang bagi siapapun secara independen untuk melakukan dan/atau menyembunyikan kesalahan atau penyimpangan dalam pelaksanaan tugas serta dapat mematikan fasilitas sistem keamanan;

c. terdapat prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*) untuk mencegah seseorang mendapat tanggung jawab atas fungsi-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;

d. bentuk pengawasan lain atau *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 (*segregation of incompatible duties)* 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, misalnya *compensating controls* antara lain *audit trail*, rekonsiliasi, *exception reporting*, *transaction log, supervisory review,* dan *independent review*.

   Sekalipun *compensating control* diterapkan, penyelenggaraan TI

tetap harus berdasarkan prinsip kehati-hatian;

e. penempatan personel mempertimbangkan kompetensi SDM, antara lain pengetahuan dan keahlian, yang sesuai dengan posisi jabatan atau tugasnya; dan

f. pembagian tanggung jawab dan penetapan target dirumuskan dengan baik di antara fungsi pengelolaan risiko dan bidang-bidang fungsional penyelenggaraan TI.

1.4. Sistem Informasi Manajemen

Dalam Pasal 7 POJK MRTI diatur bahwa komite pengarah TI bertanggung jawab memberikan rekomendasi kepada Direksi antara lain terkait kesesuaian antara TI dengan kebutuhan Sistem Informasi Manajemen (SIM) serta kebutuhan kegiatan usaha Bank sehingga Bank perlu memastikan tersedianya SIM yang dapat menghasilkan informasi yang diperlukan dalam rangka mendukung peran dan fungsi manajemen secara efektif.

Disamping itu, SIM yang dimiliki Bank harus dapat:

a. memfasilitasi pengelolaan operasional bisnis Bank termasuk pelayanan kepada nasabah;

b. mencatat dan mengumpulkan informasi secara obyektif;

c. 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;

d. meningkatkan efektivitas dan efisiensi komunikasi di Bank;

e. membantu Bank meningkatkan kepatuhan terhadap ketentuan peraturan perundang-undangan; dan

f. mendukung proses penilaian kinerja seluruh satuan kerja.

Dalam rangka memastikan efektivitas SIM, satuan kerja TI harus menetapkan kebijakan, prosedur, dan pengendalian manajemen pangkalan data (*database*) dan pembuatan laporan.

1.5. Manajemen Proyek

Dalam Pasal 11 POJK MRTI diatur bahwa Bank wajib melakukan langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan dan integrasi serta mendukung pencapaian tujuan Bank, yang mencakup penerapan manajemen proyek dalam pengembangan sistem.

Bank yang melakukan pengembangan dan pengadaan TI yang penting dan berskala besar, memerlukan suatu pengorganisasian dalam bentuk manajemen proyek. Hal ini untuk memastikan bahwa sistem TI yang diserahkan oleh satuan kerja TI kepada satuan kerja pengguna TI, telah dikembangkan dengan struktur yang baik, dan mengakomodasi kebutuhan pengguna, serta sesuai dengan sistem TI yang dimiliki Bank.

Tim manajemen proyek mengadministrasikan kemajuan masing-masing proyek dan membantu koordinasi antara pelaksana proyek dan calon pengguna sistem TI di setiap proyek, serta melaporkannya kepada komite pengarah TI. Bentuk manajemen proyek dalam organisasi Bank dapat berupa suatu satuan kerja tetap atau bersifat *ad hoc*, yang disesuaikan dengan kompleksitas dan ukuran Bank.

1.6. Rencana Strategis TI

Dalam Pasal 9 POJK MRTI, Bank wajib memiliki Rencana Strategis TI yang mendukung rencana strategis kegiatan usaha Bank dan dicantumkan dalam rencana bisnis Bank.

Rencana Strategis TI 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 Rencana Strategis TI mencakup antara lain:
    1) target perkembangan usaha Bank;
    2) standar-standar teknologi yang digunakan;
    3) ketentuan peraturan perundang-undangan yang mendasari, antara lain mengenai rahasia Bank, pengamanan, transparansi informasi produk, dan penggunaan data pribadi nasabah;
    4) rencana kebutuhan aplikasi untuk produk dan aktivitas baru serta pengembangan produk dan aktivitas yang ada;
    5) biaya terkait dengan implementasi rencana;
    6) proses yang dibutuhkan dalam rangka efisiensi;
    7) pelayanan nasabah dan kualitas kinerja teknologi;
    8) analisis kemampuan sumber daya TI yang dimiliki Bank;
    9) infrastruktur TI yang optimal untuk masa depan;

10) kemampuan untuk menyesuaikan dan mengintegrasikan dengan perkembangan teknologi baru; dan
11) kemampuan untuk menyesuaikan dengan iklim perkembangan ekonomi Indonesia secara makro.

b. Dalam penyusunan Rencana Strategis TI, Bank harus memperhatikan:
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; dan
7) rencana kebutuhan SDM.

1.7. Kebijakan, Standar, dan Prosedur Manajemen TI

Berdasarkan Pasal 8 POJK MRTI, Bank wajib memiliki dan menerapkan kebijakan, standar, dan prosedur penggunaan TI, serta wajib melakukan kaji ulang dan pengkinian kebijakan, standar, dan prosedur dimaksud secara berkala.

Disamping itu dalam Pasal 8 POJK MRTI, Bank juga wajib menetapkan jangka waktu kaji ulang dan pengkinian kebijakan, standar, dan prosedur dalam kebijakan secara tertulis.

Contoh: Bank “X” menetapkan jangka waktu kaji ulang dan pengkinian untuk kebijakan setiap 5 (lima) tahun sekali, standar setiap 2 (dua) tahun sekali, dan prosedur setiap tahun.

a. Kebijakan

Kebijakan adalah ketentuan atau prinsip yang menggambarkan

tekad, komitmen, atau rencana manajemen terhadap suatu masalah tertentu yang dinyatakan secara formal oleh manajemen, dan menjadi landasan kerja organisasi. Kebijakan untuk setiap aspek dalam pengaturan TI ini akan dijelaskan dalam bab-bab berikutnya.

Contoh : kebijakan manajemen risiko TI, kebijakan keamanan informasi, dan kebijakan penggunaan SDM TI.

b. Standar

Standar adalah seperangkat aturan teknis yang harus dipatuhi organisasi dalam rangka menerapkan suatu kerangka kerja dan tata kelola TI (dapat berasal dari intern atau ekstern). Standar menetapkan persyaratan atau ukuran tertentu yang dapat digunakan sebagai patokan bagi Bank dalam menyelenggarakan TI.

Contoh:

1) standar intern berupa standar aplikasi *desktop*, standar konfigurasi komputer, dan standar penomoran dokumen.
2) standar ekstern berupa *International Organization for Standardization* (ISO) dan Standar Nasional Indonesia (SNI).

c. Prosedur

Prosedur adalah urutan kegiatan dari suatu proses penyelenggaraan TI yang melibatkan satu atau beberapa unit kerja TI dalam Bank.

Contoh: prosedur pengendalian dokumen, pengendalian rekaman, dan audit internal.

1.8. Proses Manajemen Risiko TI

1.8.1. Identifikasi Jenis Risiko Terkait Manajemen TI

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

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

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

1.8.2. Risiko Terkait TI

Bank harus memiliki pendekatan manajemen risiko yang terpadu atau terintegrasi untuk dapat melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko secara efektif. Risiko terkait penyelenggaraan TI harus dikaji ulang bersamaan dengan risiko lainnya yang dimiliki Bank untuk menentukan profil risiko Bank secara keseluruhan. Adapun risiko terkait penyelenggaraan TI yang utama antara lain risiko operasional, risiko kepatuhan, risiko hukum, risiko reputasi, dan risiko stratejik.

1.8.3. Penilaian Risiko TI

Penilaian risiko TI oleh Bank perlu dilakukan secara berkesinambungan sebagai suatu siklus dan paling sedikit mencakup 4 (empat) langkah penting sebagai berikut:

a. Pengumpulan data atau dokumen atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko, baik dari kegiatan yang sedang maupun yang akan berjalan termasuk namun tidak terbatas pada:
   1) aset TI yang kritikal, dalam rangka mengidentifikasi titik-titik akses dan penyimpangan terhadap informasi nasabah yang bersifat rahasia;
   2) hasil kaji ulang rencana strategis bisnis, khususnya kaji ulang terhadap penilaian risiko potensial;
   3) hasil uji tuntas (*due dilligence*) dan pemantauan terhadap kinerja pihak penyedia jasa TI;
   4) hasil kaji ulang atas laporan atau keluhan yang disampaikan oleh nasabah dan/atau pengguna TI ke *call center* dan/atau *help desk;*
   5) hasil *self assessment* yang dilakukan seluruh satuan kerja terhadap pengendalian yang dilakukan terkait TI; dan
   6) temuan audit terkait penyelenggaraan dan penggunaan TI.
b. Analisis risiko berkaitan dengan dampak potensial dari setiap risiko, seperti *fraud* pada pemrograman, virus komputer,

kegagalan sistem, bencana alam, dan kesalahan pemilihan teknologi yang digunakan.

c. Penetapan prioritas pengendalian dan langkah mitigasi yang didasarkan pada hasil penilaian risiko Bank secara keseluruhan. Bank harus membuat peringkat risiko berdasarkan kemungkinan kejadian dan besarnya dampak yang dapat ditimbulkan serta mitigasi risiko yang dapat dilakukan untuk menurunkan eksposur risiko tersebut.

d. Pemantauan kegiatan pengendalian dan mitigasi yang telah dilakukan atas risiko yang diidentifikasi dalam periode penilaian risiko sebelumnya, yang antara lain mencakup rencana tindak lanjut perbaikan, kejelasan akuntabilitas dan tanggung jawab, sistem pelaporan, serta pengendalian kualitas termasuk bentuk pengawasan lain atau *compensating controls.*

1.8.4. Pengukuran Risiko Terkait TI

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 keterjadian (*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* paling sedikit mencakup:

a. penetapan aset, proses, produk, atau kejadian yang mengandung risiko;

b. pengukuran atau pemeringkatan kemungkinan kejadian dan dampak (*inherent risk assessment*);

c. langkah-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* dari manajemen, 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.

Langkah-langkah penanganan risiko potensial yang dapat diambil Bank sebagai berikut:

1) *Accept*: Manajemen 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 manajemen dan dibuat suatu sistem prosedur untuk memantau risiko tersebut, misalnya dengan menyediakan tambahan modal sesuai besarnya potensi risiko.

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*).

1.8.5. Pemantauan Risiko Terkait TI

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

a. Hal-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) pengkinian 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 *assessment* 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.

1.8.6. Pengendalian Risiko terkait TI

Manajemen harus menerapkan praktik-praktik pengendalian 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 hukum atau kontrak lainnya;
d. praktik-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 adalah kunci utama dalam proses manajemen risiko sehingga manajemen 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-aset terkait penyelenggaraan dan penggunaan TI termasuk data atau informasi;
    4) evaluasi hasil kaji ulang dan pengujian atas Rencana Pemulihan Bencana (*Disaster Recovery Plan*/DRP) untuk setiap bagian operasional yang kritis;
    5) penetapan kebijakan dan prosedur mengenai penggunaan pihak penyedia jasa TI. Direksi harus memiliki pemahaman secara menyeluruh atas risiko yang berhubungan dengan penggunaan jasa pihak penyedia jasa TI untuk sebagian atau semua operasional TI;
    6) evaluasi kemampuan penyedia jasa TI untuk menjaga tingkat keamanan paling sedikit sama atau lebih ketat dari yang diterapkan oleh pihak intern Bank baik dari sisi

kerahasiaan, integritas data, dan ketersediaan informasi. Pengawasan dan pemantauan yang ketat harus dilakukan karena tanggung jawab manajemen Bank tidak hilang atau menjadi berkurang dengan melakukan alih daya (*outsourcing*) operasional TI kepada pihak penyedia jasa TI; dan

7) pemakaian asuransi sebagai upaya untuk melengkapi mitigasi potensi kerugian dalam penyelenggaraan TI.

Risiko yang perlu diasuransikan adalah *residual risk*. Bank harus melakukan kaji ulang secara berkala atas kebutuhan, cakupan, dan nilai asuransi yang ditutup.

BAB II PENGEMBANGAN DAN PENGADAAN

2.1. Pendahuluan

Pengembangan dan pengadaan TI yang merupakan bagian dari pengelolaan TI Bank, diawali dari identifikasi dan analisis kebutuhan TI sampai dengan tahapan implementasi dan pemeliharaan TI. Pengembangan dan pengadaan TI dapat berupa pengembangan perangkat lunak secara intern atau pembelian perangkat lunak, perangkat keras, dan penggunaan jasa pengembangan sistem dari pihak lain.

Bank harus memiliki manajemen risiko yang memadai terhadap proses pengembangan dan pengadaan 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 dan pengadaan antara lain meliputi adanya kebijakan, standar, prosedur, serta proses identifikasi dan pengukuran risiko terhadap proses tersebut.

2.2. Langkah Pengendalian dalam Pengembangan dan Pengadaan

Dalam melakukan pengembangan dan pengadaan TI, Bank wajib melakukan langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan dan integrasi serta mendukung pencapaian tujuan Bank sebagaimana diatur dalam Pasal 11 POJK MRTI.

Selain langkah pengendalian sebagaimana telah diatur dalam Pasal 11 POJK MRTI, langkah pengendalian dapat juga mencakup:

a. memastikan sistem yang dikembangkan sesuai kebutuhan pengguna;
b. memastikan kesesuaian satu sistem dengan sistem yang lain agar tetap dapat berfungsi dengan baik (interoperabilitas dan kompatibilitas);
c. memiliki kode sumber atas perangkat lunak yang dikembangkan secara khusus untuk Bank yang bersangkutan (*proprietary*) sehingga kode sumber tersebut dapat diakses apabila diperlukan untuk kepentingan pemeriksaan dan penyidikan.
d. mengidentifikasi, mengukur, dan mengendalikan secara memadai atas risiko yang dapat timbul terkait dengan

pengembangan dan pengadaan TI;

e. menentukan *risk appetite* dan eksposur risiko yang dapat diterima oleh Bank terkait dengan pengembangan dan pengadaan TI;
f. memiliki prosedur pengembangan sistem dalam keadaan darurat; dan
g. memastikan adanya pemisahan lingkungan pengembangan dan operasional, termasuk memisahkan SDM yang bertanggung jawab atas proses pengembangan dengan SDM yang melakukan kegiatan operasional Bank.

2.3. Kebijakan, Standar, dan Prosedur Pengembangan dan Pengadaan

Bank wajib memiliki kebijakan, standar, dan prosedur pengembangan dan pengadaan TI sebagaimana diatur dalam Pasal 8 POJK MRTI. Proses pengembangan dan pengadaan 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. Apabila selama proses pengembangan dan pengadaan terjadi perubahan, antara lain: perubahan *user requirement* atau perubahan teknologi pendukung maka prosedur manajemen perubahan harus dirancang, dijalankan, dan didokumentasikan dengan baik.

Kebijakan, standar, dan prosedur pengembangan dan pengadaan harus memperhatikan hal-hal sebagai berikut:

a. Tahapan pengembangan TI paling sedikit meliputi:
    1) identifikasi dan analisis kebutuhan pengguna;
    2) pendefinisian kebutuhan pengguna;
    3) perancangan sistem;
    4) pemrograman;
    5) pengujian;
    6) implementasi;
    7) pengkajian ulang paska implementasi;
    8) pemeliharaan; dan
    9) pemusnahan (*disposal*).

b. Proses pengadaan TI antara lain meliputi:
   1) standar pengadaan;
   2) pedoman proyek pengadaan;
   3) *escrow agreement*;
   4) kontrak pembelian, lisensi, dan pemeliharaan perangkat lunak;
   5) pemeliharaan;
   6) garansi;
   7) penyelesaian perselisihan;
   8) perubahan perjanjian;
   9) keamanan; dan
   10) subkontrak kepada pihak lain.

c. Kebijakan, standar, dan prosedur yang perlu dimiliki Bank dalam manajemen proyek dan manajemen perubahan.

2.3.1. Kebijakan, Standar, dan Prosedur Pengembangan

2.3.1.1. Tahap Inisiasi dan Perencanaan

Tahap inisiasi terdiri dari langkah-langkah antara lain:

a. penyusunan proposal yang berisi identifikasi kebutuhan pengguna untuk menambah, menyempurnakan, atau memperbaiki suatu sistem, tujuan dan manfaat yang diharapkan, serta bagaimana sistem yang akan dikembangkan dapat mendukung strategi bisnis Bank;
b. evaluasi oleh manajemen;
c. persetujuan prinsip pengembangan sistem baru atau perubahan sistem;
d. 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;
e. persetujuan manajemen atas dokumen studi kelayakan; dan
f. penandatanganan dokumen studi kelayakan oleh semua pihak terkait.

Setelah persetujuan pengembangan diperoleh pada tahap inisiasi, Bank melakukan perencanaan untuk identifikasi lebih rinci atas aktivitas yang spesifik dan sumber daya yang dibutuhkan untuk menyelesaikan proyek. Tahap perencanaan ini menghasilkan suatu

rencana proyek yang harus menjadi acuan dalam pelaksanaan proyek dan harus dikinikan sesuai perkembangan proyek.

2.3.1.2. Tahap Pendefinisian Kebutuhan Pengguna

Berdasarkan dokumen studi kelayakan yang telah disetujui secara tertulis oleh manajemen, manajer proyek dapat membentuk tim untuk menyusun definisi kebutuhan pengguna secara detail sebagai dasar dimulainya pengembangan sistem aplikasi.

Tahap pendefinisian kebutuhan pengguna terdiri dari:

a. pengumpulan kebutuhan yang merupakan proses pengumpulan informasi, baik dengan melalui metode wawancara maupun melalui riset atau melalui 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;
b. analisis kebutuhan yang merupakan proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan. Pada tahap ini, ditentukan perkiraan umum dari waktu dan biaya pengembangan dari tiap kebutuhan dan kesesuaiannya dengan ketentuan peraturan perundang-undangan. Hasil analisis kebutuhan digunakan untuk menghasilkan alur proses bisnis, antara lain: *business process flow*, *use cases modeling* dan *data flow diagrams*, yang dapat memperjelas pemahaman mengenai kebutuhan dan solusinya, baik bagi pengguna maupun pengembang sistem;
c. 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
d. pengelolaan kebutuhan (*requirements management*) yang merupakan proses untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat

pengembangan berjalan, yang dilakukan oleh tim proyek.

2.3.1.3. Tahap Perancangan Sistem

Tahap ini mengonversikan kebutuhan informasi, fungsi, dan infrastruktur yang teridentifikasi selama tahap inisiasi dan perencanaan menjadi spesifikasi rancangan atau desain yang menjadi dasar pengembangan sistem.

Pada tahap desain diperlukan suatu standar pengendalian aplikasi yang mencakup kebijakan dan prosedur terkait dengan aktivitas pengguna dan pengendalian terintegrasi dalam sistem yang akan dikembangkan. Tahap 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.

2.3.1.4. Tahap Pemrograman

Dalam tahap ini dilakukan konversi spesifikasi desain menjadi program yang dapat dijalankan. Bank harus membuat kebijakan, standar, dan prosedur pemrograman. Selain itu, Bank harus mengkinikan rencana migrasi, implementasi, pelatihan pengguna akhir dan operator, serta dokumen manual pemeliharaan.

a. Standar Pemrograman

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

   1) membatasi akses terhadap data, program, utilitas, dan sistem di luar tanggung jawab *programmer*. Pengendalian pengelolaan *library* dapat digunakan untuk mengelola akses tersebut; dan
   2) pengendalian versi merupakan metode yang secara sistematis menyimpan kronologis dari salinan program yang disempurnakan serta menjadi salah satu dokumentasi dalam penyelenggaraan pengembangan.

b. Dokumentasi

1) 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 yaitu mencakup:
   a) deskripsi detail mengenai aplikasi;
   b) dokumentasi pemrograman berupa kode sumber, dokumen yang dapat diunduh, dan tampilan dari sistem yang dikembangkan;
   c) standar format berbagai aspek yang digunakan terkait dengan sistem seperti Pangkalan Data (*Database*), format tampilan, dan informasi;
   d) standar penamaan; dan
   e) pedoman bagi operator dan pedoman untuk pengguna akhir dalam menjalankan fungsi pada sistem secara rinci, komprehensif, dan jelas.
2) Dokumentasi harus dapat mengidentifikasikan standarisasi pengembangan, seperti narasi sistem, alur sistem, pengkodean khusus sistem, dan pengendalian intern dalam dokumen aplikasi itu sendiri.
3) Dalam hal produk atau perangkat lunak dibeli atau dikembangkan oleh pihak lain, manajemen harus memastikan kaji ulang telah dilakukan sebelumnya baik secara intern maupun oleh pihak independen bahwa dokumentasi produk atau perangkat lunak telah sesuai dengan standar minimal dokumentasi Bank.

2.3.1.5. Tahap 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:

a. *unit test*, yaitu uji coba yang dilakukan oleh pengembang atas fungsional setiap unit atau sub modul dari sistem yang telah selesai dikembangkan;
b. *system integration test* (SIT), yaitu pengujian yang dilakukan oleh pengembang terhadap keseluruhan fungsional sistem setelah diintegrasikan menjadi satu kesatuan yang utuh;
c. *stress test*, yaitu uji ketahanan yang dilakukan oleh pengembang terhadap kemampuan sistem dalam menangani proses atau transaksi dalam skala atau jumlah yang besar; dan
d. *user acceptance test* (UAT), yaitu uji coba akhir yang dilakukan oleh pengguna akhir terhadap sistem yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem, apakah telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan.

   UAT oleh pengguna akhir ini hanya dapat 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.

2.3.1.6. Tahap Implementasi

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

Hal-hal lainnya yang harus diperhatikan antara lain:

a. pengecekan integritas program berupa pengendalian yang memadai terhadap konversi dari kode sumber 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 *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 harus dihindari karena dapat mempengaruhi integritas data pada Pangkalan Data (*Database*) di *server* produksi;

g. pengaturan penyimpanan kode sumber dan Pangkalan Data (*Database*) dari sistem lama;

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.

2.3.1.7. Tahap Kaji Ulang Pascaimplementasi

Manajemen harus melakukan kaji ulang pascaimplementasi pada akhir proyek untuk mengetahui bahwa seluruh aktivitas dalam proyek telah dilaksanakan dan tujuan proyek telah tercapai. Manajemen harus menganalisis efektivitas aktivitas manajemen proyek dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek. Hasil analisis harus didokumentasikan dan dilaporkan kepada manajemen.

2.3.1.8. Tahap Pemeliharaan

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

a. *Library*

Untuk menjamin ketersediaan program yang digunakan, Bank harus memiliki *library* untuk menyimpan program. Selain itu, Bank juga perlu menyimpan informasi dan/atau dokumen berupa data dan program yang berhubungan dengan *server* atau mesin produksi yang berasal dari pengembangan dan/atau pengujian.

b. Konversi

Dalam hal terjadi *merger*, konsolidasi, atau akuisisi Bank yang memerlukan pengintegrasian sistem yang digunakan oleh Bank yang terlibat dalam *merger,* konsolidasi, atau akuisisi maka perlu dilakukan proses konversi. Dalam proses ini dilakukan modifikasi atau perubahan besar pada sistem yang ada dan pengembangan sistem baru apabila diperlukan. Dalam proses konversi ini, proses yang terstruktur seperti manajemen proyek dan siklus pengembangan sistem tetap harus diterapkan.

Mengingat kompleksitas sistem di masing-masing Bank yang terlibat *merger*, konsolidasi, atau akuisisi, diperlukan analisis secara komprehensif terhadap dampak konversi pada kegiatan operasional Bank khususnya pemrosesan transaksi. Agar proses konversi berlangsung secara efektif, Bank perlu mengantisipasi peningkatan permintaan untuk *balancing, reconcilement, exception handling*, dukungan pengguna dan nasabah, penyelesaian masalah, keterhubungan jaringan, dan sistem administrasi.

c. 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.

2.3.1.9. Tahap Pemusnahan (*Disposal*)

Setiap perangkat lunak hasil pengembangan yang sudah tidak digunakan lagi dalam kegiatan operasional dan berdasarkan pertimbangan manajemen diyakini tidak akan diperlukan dan tidak akan dipelihara lagi maka perangkat lunak tersebut akan memasuki tahap terakhir yaitu tahap pemusnahan (*disposal*). Hal ini dilakukan untuk memastikan sistem yang paling akurat dan terkini yang digunakan dalam kegiatan operasional serta menghindari penyalahgunaan oleh pihak tidak berwenang.

2.3.2. Kebijakan, Standar, dan Prosedur Pengadaan

Dalam hal sistem yang dibeli dari pihak lain melalui proses pengadaan maka perlu pula diperhatikan kesesuaian spesifikasi dengan kebutuhan, pengaruh terhadap sistem yang telah ada, dukungan teknis purna jual, kondisi keuangan perusahaan, kelengkapan dokumentasi, *escrow agreement,* dan pelatihan.

Dalam proses pengadaan sistem, Bank juga harus memastikan bahwa:

a. pengadaan perangkat keras dan perangkat lunak telah melalui studi kelayakan proyek pengadaan, mendapatkan persetujuan manajemen, terdapat pendefinisian kebutuhan pengguna, memiliki pengendalian dan pengamanan sistem yang memadai, serta terdapat pengujian dan implementasi produk; dan

b. 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:

   1) konsep dari vendor yang telah dibangun dalam bentuk purwarupa (*prototipe*) telah melewati tahap pengujian oleh sekelompok kecil pengguna operasional yang meliputi beberapa jenis peran (*business role*);

   2) pembuktian konsep dapat dilakukan secara teknis terhadap seluruh aspek teknologi yang terlibat dalam aplikasi (*steel thread*);

   3) 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

4) 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 (*stakeholder*) yang terlibat, atau batasan lainnya yang dinilai layak. Tujuan proyek percobaan ini adalah untuk menguji kinerja sistem sesuai harapan dengan membatasi risiko kerugian bagi Bank apabila terdapat kegagalan sistem.

2.3.2.1. Standar Pengadaan

Standar pengadaan harus diterapkan untuk memastikan bahwa produk yang dibeli telah memenuhi kebutuhan fungsional, kriteria keamanan, dan keandalan. Dokumen utama yang mengawali proyek pengadaan adalah *Request For Proposal* (RFP) yang paling sedikit memuat kebutuhan fungsional, keamanan, dan kebutuhan operasional secara tepat, jelas, dan terperinci.

a. Dalam pengadaan sistem, manajer proyek harus menjalankan beberapa hal penting:
   1) meninjau ulang secara menyeluruh mengenai kesesuaian vendor, kontrak, lisensi, dan produk yang diperoleh terhadap sistem yang ada;
   2) membandingkan penawaran dengan persyaratan yang ada dalam proyek dan antar sesama penawaran;
   3) mengkaji kondisi keuangan vendor dan komitmennya terhadap pelayanan; dan
   4) meminta pendapat penasihat hukum sebelum kontrak ditandatangani oleh manajemen.
b. Terkait dengan pengadaan perangkat keras, Bank memastikan

perangkat keras yang digunakan harus:

1) memenuhi aspek interkonektivitas dan kompatibilitas dengan sistem yang digunakan;
2) memperoleh sertifikat kelaikan dari Kementerian Komunikasi dan Informatika Republik Indonesia;
3) mempunyai layanan dukungan teknis, pemeliharaan, dan purnajual dari penjual atau vendor;
4) memiliki referensi pendukung dari pengguna lainnya bahwa perangkat keras tersebut berfungsi sesuai dengan spesifikasinya;
5) memiliki jaminan ketersediaan suku cadang paling sedikit 3 (tiga) tahun;
6) memiliki jaminan kejelasan tentang kondisi perangkat keras; dan
7) memiliki jaminan bebas dari cacat produk.

2.3.2.2. Pedoman Proyek Pengadaan

Proyek pengadaan harus memperhatikan paling sedikit:

a. proyek pengadaan dimulai dengan pengajuan rencana proyek kepada manajemen;
b. terdapat prosedur untuk memfasilitasi proses permintaan dan memastikan manajemen melakukan kaji ulang terhadap seluruh permintaan;
c. permintaan harus didasarkan pada kebutuhan bisnis Bank untuk:
   1) mendapatkan suatu produk, baik berupa perangkat lunak maupun perangkat keras,
   2) mengidentifikasi fitur sistem yang diinginkan, dan
   3) menggambarkan kebutuhan informasi, antarmuka jaringan (*network interface)*, serta komponen perangkat keras dan perangkat lunak;
d. Bank harus menyusun studi kelayakan untuk menentukan kebutuhan pengadaan perangkat lunak Bank, baik yang dapat dimodifikasi sesuai kebutuhan maupun yang siap pakai (*off-the shelf*);
e. persetujuan dari seluruh pihak terkait atas studi kelayakan tersebut harus didokumentasikan sebagai dasar pembuatan

definisi kebutuhan seperti yang telah dijelaskan pada sub bagian 2.3.1.2;

f. setelah Bank menerima penawaran, Bank harus menganalisis dan membandingkan penawaran antar vendor terhadap kebutuhan yang ditetapkan Bank. Proposal vendor harus membahas dengan jelas semua kebutuhan Bank dan mengidentifikasi isu-isu lain yang dapat diterapkan;

g. Bank harus memiliki prosedur untuk memastikan bahwa proses kaji ulang penawaran telah dilaksanakan dengan benar. Bank kemudian melakukan proses seleksi yang menghasilkan daftar vendor potensial;

h. manajemen harus mengkaji kembali kestabilan kondisi keuangan dan komitmen pelayanan dari vendor yang terpilih; dan

i. Bank menentukan produk dan vendor serta menegosiasikan kontrak. Satuan kerja hukum atau penasehat hukum harus meninjau ulang kontrak tersebut sebelum ditandatangani. Kontrak tersebut juga harus memuat klausul terkait pemeliharaan perangkat lunak maupun perangkat keras dalam jangka waktu tertentu, sebagai jaminan bahwa perangkat lunak maupun perangkat keras dimaksud dapat berfungsi sesuai dengan kebutuhan Bank.

2.3.2.3. *Escrow Agreement*

Dalam hal aplikasi inti dibuat oleh vendor dan kode sumber tidak diberikan kepada Bank karena aplikasinya juga digunakan oleh pihak lain (*non-proprietary*), Bank harus melindungi kepentingannya untuk menjaga kelangsungan usaha Bank. Untuk memitigasi risiko atas terhentinya dukungan vendor maka Bank harus mempertimbangkan perlu tidaknya memiliki perjanjian tertulis berupa *escrow agreement* atas aplikasi atau perangkat lunak yang dianggap penting oleh Bank. Penggunaan *escrow agreement* mempertimbangkan antara lain reputasi vendor dan berapa banyak pengguna perangkat lunak baik di dalam maupun luar wilayah Indonesia.

Dalam *escrow agreement* terdapat pihak ketiga independen yang ditunjuk untuk menyimpan kode sumber. Bank harus memastikan

paling sedikit 1 (satu) kali dalam 1 (satu) tahun bahwa pihak ketiga menyimpan versi terkini dari kode sumber. Agen penyimpanan yang dipilih harus memastikan nomor dan tanggal versi kode sumber yang disimpan dan memastikan kepada vendor mengenai integritas dari kode sumber tersebut.

2.3.2.4. Kontrak Pembelian, Lisensi, dan Pemeliharaan Perangkat Lunak

a. Lisensi Perangkat Lunak – Umum

Bank harus memastikan bahwa dalam lisensi memuat:

1) penjelasan tertulis bahwa penggunaan perangkat lunak bersifat eksklusif atau tidak;
2) informasi dan jumlah personel Bank yang dapat menggunakan perangkat lunak;
3) pembatasan lokasi penggunaan. Apabila Bank menginginkan lisensi lokasi untuk pengguna yang tidak terbatas pada suatu lokasi, harus dipastikan bahwa di dalam kontrak hal tersebut dimungkinkan;
4) daftar entitas terkait lainnya yang dapat menggunakan perangkat lunak tersebut, seperti perusahaan anak (*subsidiary*) atau perusahaan terelasi (*sister company*) Bank;
5) informasi mengenai pengembangan perangkat lunak secara *inhouse* atau alih daya (*outsourcing*) oleh vendor atau konsultan, serta pembelian perangkat lunak disertai dengan kode sumbernya, atau hanya berupa hak pakai atau sewa dengan pembatasan waktu atau fitur tertentu; dan
6) *escrow agreement* antara vendor di Indonesia dengan vendor yang ada di luar wilayah Indonesia apabila lisensi dari perangkat lunak yang digunakan Bank dengan vendor yang ada di Indonesia merupakan lisensi hak pakai yang memungkinkan adanya modifikasi berdasarkan parameter, sedangkan kode sumber perangkat lunak ada pada vendor di luar wilayah Indonesia yang tidak memiliki kontrak langsung dengan Bank.

b. Standar Spesifikasi Pengembangan dan Kinerja Perangkat Lunak

Dalam pengadaan suatu perangkat lunak, Bank harus membuat kontrak perjanjian dengan pihak penyedia jasa pengembangan

yang memuat standar spesifikasi program yang diharapkan Bank sesuai dengan kebutuhan pengguna, antara lain:

1) kinerja yang diharapkan dan fungsional dari perangkat lunak;
2) persyaratan infrastruktur yang dibutuhkan untuk menjalankan perangkat lunak;
3) identifikasi dan spesifikasi fungsional dimana perangkat lunak operasional akan bekerja dan identifikasi *milestone* dari fungsional yang harus dipenuhi oleh vendor selama proses pengembangan;
4) pengaturan izin modifikasi dari spesifikasi dan standar kinerja selama proses pengembangan;
5) identifikasi kebutuhan uji coba guna menentukan pemenuhan standar kinerja perangkat lunak;
6) tindakan yang harus dilakukan vendor jika perangkat lunak gagal pada saat uji coba;
7) jaminan keamanan dan keandalan; dan
8) penggunaan perangkat lunak untuk publik mengacu pada ketentuan peraturan perundang-undangan terkait.

2.3.2.5. Pemeliharaan

Bank perlu memperhatikan dan memastikan bahwa perjanjian lisensi atau perjanjian pengembangan memuat kesepakatan mengenai hal-hal yang diperlukan untuk pemeliharaan perangkat lunak seperti dokumentasi, modifikasi, pengkinian, dan konversi. Kesepakatan mencakup antara lain bahwa:

a. vendor memberikan pelatihan yang menyeluruh kepada personel Bank yang bertanggung jawab dalam pemeliharaan perangkat lunak;
b. vendor memberikan dokumentasi perangkat lunak, termasuk dokumentasi sistem dan petunjuk teknis penggunaan;
c. pelaksanaan dan biaya dari pengkinian dan modifikasi perangkat lunak;
d. kemungkinan Bank melakukan akses ke kode sumber bila vendor tidak dapat memberikan layanan lagi atau terdapat kebutuhan modifikasi yang tidak dapat dilakukan oleh vendor; dan

e. kemungkinan vendor untuk membantu proses konversi data pada saat penggantian sistem pada masa mendatang paling sederhana dalam format standar seperti format *text*.

Dalam hal diperlukan, kesepakatan tersebut dapat dimuat dalam suatu perjanjian pemeliharaan yang tersendiri.

2.3.2.6. Garansi

Bank perlu melakukan penelitian untuk meyakini terdapat jaminan bahwa lisensi perangkat lunak dari vendor:

a. tidak melanggar hak kekayaan intelektual dari pihak lainnya di seluruh dunia;
b. tidak mengandung kode rahasia, pembatasan yang tidak diungkapkan, atau pembatasan secara otomatis pada perjanjian;
c. berfungsi sesuai spesifikasi dan harus dinyatakan batasan tanggung jawab vendor dalam hal terjadi permasalahan;
d. pemeliharaannya dilakukan oleh vendor selama jangka waktu yang diperjanjikan; dan
e. tetap berlaku dalam hal terjadi penggabungan, peleburan, pengambilalihan, atau perubahan kepemilikan baik pada Bank atau vendor.

2.3.2.7. Penyelesaian Perselisihan

Bank harus memasukkan klausula penyelesaian perselisihan pada perjanjian lisensi. Pemahaman mengenai klausula tersebut akan meningkatkan kemampuan Bank untuk menyelesaikan permasalahan dengan cara terbaik dan memungkinkan untuk meneruskan pengembangan perangkat lunak selama periode penyelesaian perselisihan.

2.3.2.8. Perubahan Perjanjian

Bank harus memastikan bahwa pada lisensi perangkat lunak secara jelas menyatakan bahwa vendor tidak dapat memodifikasi perjanjian tanpa adanya persetujuan dari kedua belah pihak.

2.3.2.9. Keamanan

Bank harus menetapkan kriteria pengendalian keamanan (*security control*) atas TI yang akan menjadi standar kinerja dari fitur keamanan dalam perjanjian lisensi dan perjanjian pengembangan perangkat lunak. Standar tersebut harus memastikan bahwa

perangkat lunak yang dikembangkan konsisten dengan keseluruhan program keamanan yang ada di Bank. Perjanjian lisensi dan pengembangan tersebut antara lain mencakup:

1) tanggung jawab terus menerus dari pihak vendor untuk melindungi keamanan dan kerahasiaan sumber daya dan data Bank;
2) larangan bagi vendor untuk menggunakan atau mengungkapkan informasi yang dimiliki Bank tanpa persetujuan Bank;
3) jaminan dari vendor bahwa perangkat lunak tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam sistem dan data Bank; dan
4) pernyataan secara eksplisit bahwa vendor tidak akan menggunakan fitur yang dapat mengakibatkan perangkat lunak tidak berfungsi dengan baik.

2.3.2.10. Subkontrak kepada Vendor

Bank harus menetapkan klausula dalam perjanjian pengembangan yang melarang penugasan kontrak oleh vendor kepada pihak ketiga tanpa persetujuan Bank. Apabila memang terdapat kondisi dimana sebagian dari pengembangan perangkat harus disubkontrakkan maka harus terdapat persetujuan tertulis dari Bank. Dalam memberikan persetujuan subkontrak tersebut, Bank harus mempertimbangkan tingkat kesulitan dan ketersediaan ahli dalam pengembangan perangkat lunak tersebut serta keamanan data Bank. Disamping itu, Bank harus memastikan terdapat klausula yang menyatakan bahwa vendor bertanggung jawab terhadap perangkat lunak meskipun dirancang atau dikembangkan oleh pihak lain.

2.3.3. Kebijakan, Standar, serta Prosedur Manajemen Proyek dan Manajemen Perubahan

a. Manajemen proyek perlu memperhatikan antara lain:
    1) Bank harus melakukan studi kelayakan untuk mengetahui biaya dan manfaat dari pengembangan dan pengadaan TI, sekaligus untuk menentukan penggunaan sumber daya intern atau alih daya (*outsourcing*) kepada vendor;
    2) Bank harus menspesifikasikan secara jelas persyaratan

keamanan yang relevan sebelum sistem baru dikembangkan atau dibeli. Persyaratan keamanan tersebut harus sesuai dengan arsitektur keamanan informasi Bank secara keseluruhan;

3) Bank harus melakukan perencanaan yang baik untuk memastikan bahwa tujuan proyek akan tercapai;
4) Bank harus melakukan klasifikasi pemisahan lingkungan untuk pengembangan, uji coba, dan produksi, termasuk pembatasan akses ke masing-masing bagian lingkungan;
5) Bank harus memastikan kecukupan pelatihan dan kejelasan petunjuk penggunaan sistem informasi yang disusun sebagai bagian dari kontrak antara Bank dengan vendor;
6) terhadap sistem yang didukung atau dipelihara oleh vendor, harus terdapat analisis pemilihan perangkat lunak yang memadai sehingga memastikan kebutuhan pengguna dan proses bisnis terpenuhi;
7) terdapat perjanjian secara tertulis antara Bank dengan vendor;
8) Bank harus menerapkan manajemen pemeliharaan untuk semua proses pengembangan dan pengadaan yang telah diimplementasikan;
9) seluruh hasil (*deliverables*) pada setiap tahapan manajemen proyek harus didokumentasikan dengan baik; dan
10) Bank harus memiliki rencana proyek yang formal meliputi:
    a) identifikasi proyek, sponsor, dan manajer proyek;
    b) tujuan proyek, informasi latar belakang, dan strategi pengembangan;
    c) deskripsi tugas dan tanggung jawab utama dari tiap personel dalam manajemen proyek;
    d) prosedur untuk mengumpulkan dan menyebarkan informasi;
    e) kriteria hasil yang ditargetkan dapat diterima untuk masing-masing tahap pengembangan;
    f) masalah keamanan dan pengendalian yang harus dipertimbangkan;

g) prosedur untuk memastikan manajer proyek menilai, mengawasi, serta mengatur risiko intern dan ekstern dengan benar sepanjang siklus pengembangan;
h) tanggal akhir pemberlakuan (*cut off date)* untuk mengalihkan penggunaan sistem aplikasi dari yang lama ke versi terbaru hasil pengembangan atau perubahan;
i) standar pengembangan yang akan digunakan untuk pengawasan proyek, pengendalian sistem, dan kendali mutu;
j) jenis dan tingkatan dokumentasi yang harus dihasilkan oleh setiap personel di setiap tahapan proyek;
k) jadwal tahapan proyek dan aktivitas yang akan diselesaikan dalam tiap tahap;
l) estimasi anggaran awal dari keseluruhan biaya proyek;
m) rencana uji coba yang mengidentifikasikan kebutuhan uji coba berdasarkan jenis, prosedur, dan jadwal uji coba; dan
n) rencana pelatihan yang mengidentifikasikan kebutuhan dan jadwal pelatihan agar pegawai Bank dapat menggunakan dan memelihara aplikasi pascaimplementasi.

b. Proses manajemen perubahan paling sedikit mencakup:
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 sebelum modifikasi;
4) dokumentasi yang terdiri atas:
a) penjelasan dari modifikasi,
b) alasan dari penerapan atau penolakan dari modifikasi yang diusulkan,
c) nama individu yang membuat modifikasi,
d) salinan dari kode sumber yang diubah,
e) tanggal dan waktu modifikasi dilakukan, dan

f) evaluasi setelah modifikasi; dan

5) dokumentasi yang harus dibuat selama proses modifikasi berlangsung terdiri atas:
   a) informasi yang menjadi prioritas,
   b) identifikasi sistem, Pangkalan Data (*Database*), dan satuan kerja yang terpengaruh,
   c) nama dari individu yang bertanggung jawab dalam membuat perubahan,
   d) kebutuhan sumber daya,
   e) prediksi biaya,
   f) prediksi tanggal penyelesaian,
   g) prediksi tanggal implementasi,
   h) pertimbangan potensi keamanan dan keandalan modifikasi sistem,
   i) kebutuhan uji coba,
   j) prosedur implementasi,
   k) perkiraan *downtime* pada saat implementasi,
   l) prosedur rekam cadang (*backup*),
   m) pengkinian dokumentasi, antara lain berupa rancangan program dan *script*, topologi jaringan, manual pengguna, dan rencana kontinjensi,
   n) dokumentasi penerimaan modifikasi dari semua satuan kerja terkait, antara lain berupa pengguna, teknologi, *quality assurance*, keamanan, audit, dan
   o) dokumentasi audit pascaimplementasi disertai dengan perbandingan antara harapan dan hasil.

2.4. Proses Manajemen Risiko Pengembangan dan Pengadaan

2.4.1. Pengukuran Risiko terkait Pengembangan dan Pengadaan

Pengukuran tingkat risiko pada proses pengembangan dan pengadaan TI tergantung pada faktor terkait antara lain:

a. kesesuaian dengan rencana strategis bisnis dan regulasi yang berlaku;
b. adanya perubahan pada cakupan sistem atau proses;
c. pemisahan lingkungan pengembangan, uji coba dan operasional, termasuk pengaturan aksesnya kepada pengembang, penguji, dan pengguna;

d. rencana sistem aplikasi yang akan diperoleh melalui pembelian paket tanpa modifikasi, pembelian paket dengan modifikasi, pengembangan sendiri secara intern atau oleh pihak ketiga;
e. cakupan dan tingkat kekritisan sistem atau banyaknya unit bisnis yang terpengaruh;
f. kompleksitas tipe pemrosesan dari aplikasi yang akan dikembangkan (*batch, real-time, client* atau *server, parallel distributed*);
g. volume dan nilai transaksi dari sistem aplikasi yang akan dikembangkan;
h. klasifikasi dan sensitivitas data dari sistem yang akan dikembangkan;
i. dampak pada data (baca (*read*), unduh (*download*), unggah (*upload*), pengkinian (*update*), atau ubah (*alter*));
j. tingkat pengalaman dan kemampuan vendor, jika sistem dibeli atau dikembangkan oleh pihak ketiga;
k. kecukupan jumlah dan kemampuan personel yang termasuk dalam tim pengembangan;
l. kesesuaian *platform* dan aplikasi yang dipilih dengan arsitektur Bank;
m. ketergantungan sistem yang dikembangkan dengan sistem yang telah ada;
n. ketidaksesuaian jumlah pengguna dengan rencana awal pengembangan atau terdapat perubahan struktur organisasi saat proses pengembangan;
o. perubahan ketentuan;
p. adanya risiko baru atau risiko yang dapat muncul dari teknologi yang sedang dikembangkan atau risiko keusangan teknologi;
q. adanya kelemahan audit atau kelemahan yang ditemui dalam *self-assessment*; dan
r. ketidaksesuaian pelaksanaan pengembangan dengan target waktu penyelesaian.

2.4.2. Pengendalian Risiko Pada Pengembangan dan Pengadaan

Pada setiap tahapan pengembangan dan pengadaan TI, Bank harus memitigasi risiko yang telah diidentifikasi dan diukur dengan beberapa cara pengendalian yang telah ditetapkan dalam kebijakan,

standar, dan prosedur pengembangan dan pengadaan TI Bank. Setelah melakukan mitigasi, Bank harus memantau risiko yang dikendalikan dan *residual risk* karena setiap gangguan yang dapat mempengaruhi rencana dan proses pengembangan dan pengadaan TI, pada akhirnya dapat berdampak pada kegiatan operasional Bank.

2.4.2.1. Pengendalian Risiko pada Pengembangan

Dalam rangka mengendalikan risiko terkait pengembangan TI, Bank harus dapat memastikan bahwa pengembangan sistem yang dilakukan telah sesuai dengan kebijakan, standar, dan prosedur untuk setiap tahapan pengembangan. Hal ini dilakukan dengan memperhatikan:

a. rencana pengembangan sistem telah sesuai dengan kebutuhan pengguna dan arah kebijakan bisnis Bank;

b. rancangan sistem yang dikembangkan telah mencakup kebutuhan pengguna pada tahap inisiasi dan perencanaan serta sesuai dengan standar pengendalian aplikasi yang melibatkan partisipasi dari audit intern.

   Berdasarkan tujuannya, pengendalian terbagi atas pengendalian yang bersifat pencegahan, deteksi atau temuan, atau koreksi. Pengendalian yang harus dilakukan paling sedikit meliputi:

   1) Pengendalian *Input*

      Paling sedikit mencakup pengecekan terhadap validitas atau kebenaran data, *range* data, parameter, dan duplikasi data yang di-*input*;

   2) Pengendalian Proses

      Memastikan proses bekerja secara akurat dan dapat menyimpan atau menolak informasi. Pengendalian proses yang dapat dilakukan secara otomatis oleh sistem mencakup paling sedikit *error reporting*, *transaction log*, pengecekan urutan, dan rekam cadang (*backup*) *file*; dan

   3) Pengendalian *Output*

      Memastikan sistem mengelola informasi dengan aman dan mendistribusikan informasi hasil proses dengan tepat serta menghapus informasi yang telah melewati masa retensi;

c. hasil pemrograman dibangun berdasarkan spesifikasi desain dengan dilakukannya rencana uji coba yang didokumentasikan

untuk mempermudah penelusuran pengubahan sistem aplikasi;

d. pelaksanaan rangkaian uji coba dengan menetapkan ruang lingkup tes skenario, penilaian atas hasil uji coba, melakukan perbaikan pada sistem sampai dengan mendapatkan pengesahan atas laporan hasil uji coba;

e. implementasi sistem yang baru dapat berjalan dengan sistem yang lama dengan adanya persiapan instalasi, migrasi *file*, konversi data, dokumen petunjuk teknis, dan pelatihan; dan

f. hasil implementasi dari sistem berjalan dengan baik secara berkesinambungan dengan dilakukannya kaji ulang secara berkala atas hasil efektivitas pemeliharaan.

2.4.2.2. Pengendalian Risiko pada Pengadaan

Dalam rangka mengendalikan risiko pada pengadaan, Bank harus membuat kriteria pemilihan vendor dan melakukan kaji ulang kemampuan vendor antara lain terkait dengan kondisi keuangan, tingkat dukungan (*support level*), dan pengendalian keamanan, sebelum menetapkan pilihan produk atau layanan dari vendor.

Bank harus melakukan kaji ulang perjanjian lisensi (*licensing agreement*) untuk memastikan hak dan tanggung jawab masing-masing pihak secara jelas dan wajar. Penasihat hukum Bank harus melakukan konfirmasi bahwa jaminan kinerja (*performance guarantee*), akses terhadap kode sumber, hak cipta, dan keamanan perangkat lunak atau data, telah diatur secara jelas sebelum pihak manajemen menandatangani perjanjian. Hal-hal yang perlu diperhatikan adalah:

a. memastikan proses pengadaan telah sesuai dengan kebijakan, standar, dan prosedur Bank serta ketentuan berlaku terkait pengadaan; dan

b. melakukan segala perikatan yang memiliki kekuatan hukum secara memadai.

BAB III AKTIVITAS OPERASIONAL TI

3.1. Pendahuluan

Perkembangan TI memungkinkan Bank menjalankan kegiatan operasional yang semakin kompleks. Operasional TI tidak hanya terkonsentrasi di Pusat Data tetapi juga pada aktivitas lain yang terkait dengan penggunaan aplikasi yang terintegrasi, beragam media komunikasi, koneksi internet, dan berbagai *platform* komputer. Sementara itu, akses *input* dan *output* dapat dilakukan oleh banyak pengguna dari berbagai lokasi. Demikian juga dengan pemrosesan, dapat dilakukan di berbagai lokasi yang berjauhan namun saling terkait, baik secara *real-time online,* daring (*online*), maupun luring (*offline*). Oleh karena itu, diperlukan pengendalian yang memadai atas operasional TI agar Bank dapat meminimalisasi risiko terganggunya kerahasiaan, integritas, dan ketersediaan informasi.

Pengaturan atas aktivitas operasional TI yang memadai sangat penting untuk memastikan informasi pada sistem telah lengkap, akurat, terkini, terjaga integritasnya, dan andal, serta terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan, dan perusakan data.

3.2. Kebijakan, Standar, dan Prosedur terkait Aktivitas Operasional TI

Sesuai Pasal 12 POJK MRTI, Bank wajib memastikan kelangsungan dan kestabilan operasional TI serta memitigasi risiko yang berpotensi dapat mengganggu kegiatan operasional Bank.

Bank harus memiliki kebijakan yang mencakup setiap aspek operasional TI dan disesuaikan dengan kompleksitas operasional TI Bank. Aspek operasional TI antara lain meliputi Pusat Data, perencanaan dan pemantauan kapasitas, pengelolaan konfigurasi perangkat keras dan perangkat lunak, serta pengelolaan Pangkalan Data (*Database*).

Prosedur memuat tanggung jawab, akuntabilitas, pemberian wewenang, dan pedoman bagi para pelaksana kegiatan operasional. Selain itu, manajemen harus menetapkan standar perangkat keras dan perangkat lunak yang dipergunakan di lingkungan operasional, pengujian, dan pengembangan dalam penyelenggaraan TI Bank.

3.2.1. Kebijakan terkait Pusat Data

Dalam Pasal 22 POJK MRTI, Pusat Data dan Pusat Pemulihan Bencana wajib menjamin kelangsungan usaha Bank.

a. 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:

1) penjadwalan tugas

Bank memiliki dan melaksanakan jadwal semua tugas yang harus dijalankan di Pusat Data operasional TI secara efektif dan aman dari perubahan yang tidak sah;

2) pengoperasian tugas

Pemberian akses *command line* kepada operator TI harus dibatasi sesuai kewenangan pada fungsi pengoperasian tugas yang telah ditentukan;

3) pendistribusian *output*

Hasil informasi yang diproduksi oleh sistem (*output*), dalam bentuk *softcopy* atau *hardcopy*, dapat merupakan informasi yang sensitif atau rahasia. Prosedur yang harus dimiliki Bank meliputi penentuan informasi yang akan diproduksi, pendistribusian *output* baik secara fisik maupun *logic*, dan pemusnahan (*disposal*) *output* yang sudah tidak diperlukan lagi. Prosedur tersebut diperlukan untuk menghindari terbukanya informasi yang bersifat rahasia dan meningkatnya biaya akibat adanya *output* yang tidak diperlukan, serta untuk memastikan keamanan *output*;

4) proses rekam cadang (*backup*) baik *onsite* maupun *offsite, restore,* unduh (*download*), dan unggah (*upload*) untuk Pangkalan Data (*Database*);

5) pemantauan perangkat keras dan perangkat lunak; dan

6) pengaktifan jejak audit (*audit trail*).

b. Pengendalian Akses Fisik Pusat Data

Akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik. Pintu Pusat Data harus selalu terkunci dan dilengkapi dengan kartu akses dan/atau *biometric device*. Ruang Pusat Data 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.

c. Pengendalian Lingkungan Pusat Data

Kondisi lingkungan pemrosesan TI yang tidak sesuai standar dapat menimbulkan gangguan pada operasional TI sehingga manajemen paling sedikit:

1) mengawasi dan memantau faktor lingkungan 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);
2) memastikan tersedianya sumber listrik yang cukup, stabil, dan tersedianya sumber alternatif listrik untuk mengantisipasi tidak berfungsinya 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;
3) 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;
4) menggunakan lantai yang ditinggikan (*raised floor)* untuk mengamankan sistem perkabelan dan menghindari efek *grounding* di Pusat Data; dan

5) menginventarisasi perangkat pendukung Pusat Data antara lain UPS dan *power control, fire detection and extinguisher*, *air conditioning*, termometer, dan higrometer.

3.2.2. Kebijakan Perencanaan dan Pemantauan Kapasitas TI

Bank perlu memiliki kebijakan dan prosedur perencanaan dan pemantauan kapasitas TI untuk dapat memastikan bahwa perangkat keras dan perangkat lunak yang digunakan Bank telah sesuai dengan kebutuhan operasional bisnis dan mengantisipasi perkembangan usaha Bank. Tanpa perencanaan kapasitas TI yang baik, Bank dapat menghadapi risiko kekurangan atau bahkan pemborosan sumber daya TI. Perencanaan kapasitas TI harus disusun untuk jangka waktu cukup panjang dan selalu dikinikan untuk mengakomodasi perubahan yang ada.

3.2.3. Kebijakan Pengelolaan Konfigurasi Perangkat Keras dan Perangkat Lunak

Bank harus menetapkan prosedur terkait:

a. proses instalasi perangkat keras dan perangkat lunak;
b. pengaturan parameter (*hardening*) perangkat keras dan perangkat lunak; dan
c. inventarisasi dan pengkinian informasi perangkat keras, perangkat lunak, infrastruktur jaringan, media penyimpan, dan perangkat pendukung lainnya yang terdapat di Pusat Data. Inventarisasi yang dilakukan meliputi:
   1) Perangkat keras

      Inventarisasi perangkat keras harus dilakukan secara menyeluruh termasuk inventarisasi terhadap perangkat keras yang dimiliki oleh pihak lain tetapi berada di Bank. Informasi penting yang harus dicakup dalam inventarisasi perangkat keras antara lain nama vendor dan model, tanggal pembelian dan instalasi, kapasitas *processor*, memori utama, kapasitas penyimpanan, sistem operasi, fungsi, dan lokasi.
   2) Perangkat lunak

      Bank harus melakukan inventarisasi atas 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 meliputi nama vendor, tanggal instalasi, nomor versi dan keluaran (*release*), pemilik perangkat lunak, s*etting* parameter dan *service* yang aktif, jumlah lisensi yang dimiliki, jumlah perangkat lunak yang di-*install,* dan jumlah pengguna.

3) Infrastruktur jaringan

Infrastruktur jaringan merupakan hal yang penting bagi operasional Bank sehingga manajemen harus mendokumentasikan secara lengkap konfigurasi jaringan. Informasi yang harus dicakup antara lain:

a) diagram jaringan;
b) identifikasi seluruh koneksi intern dan ekstern Bank;
c) daftar dan kapasitas peralatan jaringan seperti *switch, router, hub, gateway,* dan *firewall*;
d) identifikasi vendor telekomunikasi;
e) rencana perluasan dan perubahan konfigurasi jaringan; dan
f) gambaran sistem pengamanan jaringan.

4) 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, *source system*, serta frekuensi dan masa retensi rekam cadang (*backup*).

3.2.4. Kebijakan Pemeliharaan Perangkat Keras dan Perangkat Lunak

a. Pemeliharaan Perangkat Keras

Pemeliharaan preventif secara berkala terhadap peralatan TI perlu dilakukan untuk meminimalisasi kegagalan pengoperasian peralatan tersebut dan untuk mendeteksi secara dini permasalahan yang potensial. Untuk itu Bank perlu memiliki perjanjian pemeliharaan dengan vendor guna memastikan ketersediaan dukungan pemeliharaan dari vendor. Pemeliharaan didasarkan jadwal yang telah ditetapkan, didokumentasikan pada suatu *log-book*, dan dilakukan kaji ulang secara berkala.

b. Pemantauan Kinerja Perangkat Keras dan Perangkat Lunak

Pemantauan terhadap perangkat keras dan perangkat lunak dilakukan setiap hari untuk memastikan seluruh perangkat tersebut beroperasi sebagaimana mestinya.

Misalnya *server* tetap dalam keadaan menyala, kapasitas Pangkalan Data (*Database*) dan utilitas *server* tidak melampaui limit, dan fasilitas pendukung berfungsi dengan baik.

3.2.5. Kebijakan Manajemen Perubahan (*Change Management*)

Manajemen perubahan adalah prosedur yang mengatur penambahan, penggantian, maupun penghapusan obyek di lingkungan operasional. Obyek dimaksud dapat berupa data, program, menu, aplikasi, perangkat komputer, perangkat jaringan, dan proses.

Bank harus memiliki kebijakan, standar, dan prosedur manajemen perubahan yang paling sedikit mencakup permintaan, analisis, persetujuan perubahan, dan instalasi perubahan termasuk pemindahan perangkat keras dan perangkat lunak dari lingkungan pengujian ke lingkungan operasional.

Manajemen perubahan harus memperhatikan:

a. 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*.

b. *Patch management*

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 terbaru yang paling sesuai. 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.

c. 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*.

3.2.6. 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 perangkat keras, sistem operasi, sistem aplikasi, perangkat jaringan, dan peralatan keamanan.

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

a. Pengelolaan *Helpdesk*

Bank harus memiliki fungsi *helpdesk* agar Bank dapat menanggapi dan menangani permasalahan yang dihadapi oleh seluruh pengguna di Bank dengan segera. Bank akan menghadapi risiko jika tidak memiliki prosedur *helpdesk* yang memadai untuk memastikan bahwa pengguna telah memperoleh solusi atas permasalahan yang dihadapi.

Hal-hal yang perlu diperhatikan dalam fungsi *helpdesk* adalah:

1) Tersedianya dokumentasi permasalahan yang lengkap

Dokumentasi permasalahan harus mencakup data pengguna, penjelasan masalah, dampak pada sistem (*platform*, aplikasi, atau lainnya), kode 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 lainnya.

2) Sistem *helpdesk*

Bank perlu menggunakan sistem yang dapat memberikan bantuan kepada staf *helpdesk* tentang alternatif solusi permasalahan yang umum terjadi. Bank secara berkala melakukan pengkinian terhadap sistem tersebut dengan informasi yang didapat dari vendor dan dari pengalaman staf *helpdesk*.

b. Pengelolaan *Power User*

Power user adalah *user id* yang memiliki kewenangan sangat luas. Dalam rangka penanganan permasalahan, Bank menetapkan prosedur penanganan *power user* agar penggunaannya tidak disalahgunakan. Prosedur tersebut antara lain mengatur:

1) penetapan pihak yang memiliki hak akses *power user* termasuk penerapan *dual custody* (pemecahan *password* kepada lebih dari 1 (satu) orang);
2) prosedur penyimpanan *password power user*;
3) prosedur *break ID power user* pada keadaan darurat;
4) prosedur penggantian *password power user* setelah digunakan; dan
5) pendokumentasian penggunaan *power user* dalam bentuk berita acara.

3.2.7. Kebijakan 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 pengawasan. 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*) adalah pengaksesan, pemeliharaan, penanganan permasalahan, dan administrasi Pangkalan Data (*Database*).

3.2.8. Kebijakan 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:

a. permintaan dan pemberian informasi oleh pihak intern dan ekstern; dan
b. pengiriman informasi melalui berbagai media, seperti *hardcopy*, *tape*, *disk*, *email*, pos, dan internet.

Pada Bank besar dengan kompleksitas TI yang tinggi, manajemen 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.

3.2.9. Kebijakan Pengelolaan *Library*

Pengelola *library* bertanggung jawab untuk menginventarisasi dan menyimpan seluruh perangkat lunak dan data yang tersimpan dalam berbagai media, antara lain *tape* dan *disk*. Disamping itu, pengelola *library* juga menyimpan salinan dari seluruh kebijakan dan prosedur seperti *run book manual* terkait Pusat Data.

Adapun prosedur yang harus ditetapkan antara lain:

a. pengamanan akses ke data di *library*;
b. penanganan media penyimpan data (untuk Pangkalan Data (*Database*) dan *audit journal*);
c. masa retensi media penyimpan data;

d. pengujian media penyimpan data; dan

e. keluar dan masuk media penyimpan data dari dan ke *library*.

Dalam membuat kebijakan, standar, dan prosedur untuk *library*, 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 lainnya.

3.2.10. Kebijakan Pemusnahan (*Disposal*) Perangkat Keras dan Perangkat Lunak

Pemusnahan (*Disposal*) meliputi penghapusan perangkat lunak, perangkat keras, dan data yang sudah tidak digunakan lagi atau yang masa retensinya telah habis. Kode sumber versi lama yang sudah tidak dipakai lagi harus disimpan dengan informasi yang jelas mengenai tanggal, waktu, dan informasi lain ketika digantikan dengan kode sumber versi terbaru. Kegiatan yang dilakukan meliputi antara lain:

a. memindahkan data dari sistem produksi ke media rekam cadang (*back-up*) dengan mekanisme sesuai prosedur, termasuk prosedur uji coba dan rekam cadang (*back-up*);

b. menyimpan dokumentasi sistem sebagai persiapan jika diperlukan untuk meng-*install* ulang suatu sistem ke *server* produksi;

c. mengelola arsip data sesuai masa retensi; dan

d. memusnahkan data yang habis masa retensinya.

3.3. Proses Manajemen Risiko Aktivitas Operasional TI

Manajemen risiko aktivitas operasional TI harus memperhatikan:

a. Kejadian atau aktivitas yang dapat mengganggu operasional antara lain:

   1) kesalahan investasi teknologi termasuk penerapan yang tidak benar, kegagalan dari pihak vendor, pendefinisian dari kebutuhan bisnis yang tidak tepat, ketidaksesuaian dengan sistem-sistem yang ada, atau keusangan perangkat lunak, termasuk hilangnya dukungan vendor terhadap perangkat keras dan perangkat lunak yang digunakan oleh Bank;

2) permasalahan pengembangan sistem dan implementasi termasuk ketidakcukupan manajemen proyek, biaya dan waktu yang melebihi batas, *error* pada pemrograman, kegagalan untuk mengintegrasikan atau migrasi dari sistem yang ada, atau kesalahan dari sebuah sistem untuk memenuhi kebutuhan pengguna;
3) permasalahan pada kapasitas sistem seperti kekurangan pada perencanaan kapasitas, ketidakcukupan kapasitas untuk mengakomodasi fleksibilitas sistem, dan/atau ketidakcukupan perangkat lunak untuk mengakomodasi pengembangan bisnis;
4) kegagalan sistem termasuk pada jaringan, *interface*, perangkat keras, perangkat lunak, atau kegagalan komunikasi intern; dan
5) pelanggaran pada keamanan sistem termasuk pelanggaran pada keamanan ekstern dan intern, penipuan dalam pemrograman, atau virus pada komputer.

b. Tingkat risiko operasional TI yang tergantung pada faktor terkait antara lain:
1) kesesuaian dengan rencana strategis bisnis dan regulasi yang berlaku;
2) perubahan pada cakupan sistem atau proses;
3) lokasi pengaksesan sistem (intern atau ekstern, termasuk internet, *dial-up*, atau WAN);
4) perolehan aplikasi antara lain melalui pembelian paket tanpa modifikasi, pembelian paket dengan modifikasi, dan/atau pengembangan sendiri secara intern atau oleh pihak ketiga;
5) cakupan dan tingkat kekritisan sistem atau banyaknya unit bisnis yang terpengaruh;
6) kompleksitas tipe pemrosesan dari aplikasi (*batch, realtime, client* atau *server,* atau *parallel distributed*);
7) volume dan nilai transaksi dari sistem;
8) klasifikasi dan sensitivitas data yang diproses atau digunakan;
9) dampak pada data (baca (*read*), unduh (*download*), unggah (*upload*), pengkinian (*update*), atau ubah (*alter*));

10) tingkat pengalaman dan kemampuan pengelola TI;
11) kecukupan jumlah dan kemampuan staf pelaksana;
12) keragaman *platform*, aplikasi, dan *delivery channel*;
13) jumlah pengguna dan nasabah;
14) perubahan ketentuan;
15) adanya risiko baru atau risiko yang dapat muncul dari teknologi yang sedang dikembangkan atau risiko keusangan teknologi; dan
16) adanya kelemahan audit atau kelemahan yang ditemui dalam *self-assessment*.

BAB IV JARINGAN KOMUNIKASI

4.1. Pendahuluan

Perkembangan teknologi jaringan komunikasi telah mengubah pendekatan usaha Bank menjadi tanpa mengenal batasan waktu dan tempat. Bank dapat menyediakan layanan perbankan secara *realtime online* dari seluruh kantor dan *delivery channel* lainnya, seperti; *Automated Teller Machine* (ATM), *internet banking, mobile banking*, dan *Electronic Data Capture* (EDC), baik milik Bank maupun milik pihak penyedia jasa TI.

Jaringan komunikasi mencakup perangkat keras, perangkat lunak, dan media transmisi yang digunakan untuk mentransmisikan informasi berupa data, suara (*voice*), gambar (*image*), 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.

4.2. Kebijakan, Standar, dan Prosedur terkait Jaringan Komunikasi

Dalam Pasal 13 POJK MRTI, Bank wajib menyediakan jaringan komunikasi yang memenuhi prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Untuk memenuhi kewajiban tersebut, Bank harus memiliki kebijakan, standar, dan prosedur sebagai pedoman dalam menyediakan jaringan komunikasi untuk meyakinkan 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) pada

layer Session.

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

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

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, and 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 *recovery*; dan
h. perjanjian dan SLA yang sesuai dengan kebutuhan Bank dan dipantau secara berkala apabila jaringan komunikasi yang digunakan oleh Bank diselenggarakan oleh pihak penyedia jasa TI.

4.3. Proses Manajemen Risiko Jaringan Komunikasi

4.3.1. Pengendalian Risiko

a. Penggunaan teknologi jaringan komunikasi memberikan berbagai kemudahan dan manfaat bagi Bank dan nasabah, namun demikian, perlu diperhatikan risiko-risiko yang mungkin timbul, antara lain:
    1) kehilangan data/informasi;
    2) kehilangan integritas data/informasi;
    3) tidak lengkapnya data/informasi yang ditransmisikan;
    4) hilangnya kerahasiaan informasi;
    5) tidak tersedianya jaringan komunikasi akibat gangguan atau bencana; dan
    6) kehilangan/kerusakan perangkat jaringan komunikasi.
b. Dalam mengendalikan risiko pada jaringan komunikasi, Bank harus memperhatikan hal-hal sebagai berikut:
    1) Desain Jaringan Komunikasi

Jaringan komunikasi harus didesain sedemikian rupa sehingga efisien tetapi juga dinamis untuk mengantisipasi pengembangan di masa mendatang. Pada tahap ini, terdapat beberapa hal yang perlu diperhatikan, yaitu:

a) penentuan topologi jaringan komunikasi;
b) perencanaan kapasitas (*capacity planning*) jaringan komunikasi;
c) pemilihan media jaringan komunikasi;
d) rekam cadang (*backup*) perangkat keras, jalur alternatif (*alternative routing*), atau *provider* alternatif;
e) pengamanan fisik dan *logic*:
    i. penempatan perangkat jaringan pada lokasi yang aman terhadap gangguan alam dan akses oleh orang yang tidak berhak; dan
    ii. pengaturan parameter sistem perangkat jaringan.
f) tersedianya jejak audit, paling sedikit untuk perubahan-perubahan pada *setting* parameter dan hak akses perangkat jaringan komunikasi dan juga penggunaan atas hak akses tersebut.

2) Pengendalian Akses

Pengendalian akses di jaringan komunikasi sangat penting dan harus diperhatikan karena jaringan komunikasi merupakan pintu utama untuk masuk ke dalam sistem informasi Bank. Jika tidak dikelola dengan baik, maka keamanan informasi menjadi terancam. Dalam menerapkan pengendalian akses, terdapat beberapa hal yang harus diperhatikan oleh Bank, yaitu:

a) akses ke jaringan komunikasi oleh pengguna didasarkan pada kebutuhan bisnis dengan memperhatikan aspek keamanan informasi;
b) melakukan pemisahan jaringan komunikasi berdasarkan segmen baik secara fisik maupun *logic,* misalnya pemisahan antara lingkungan pengembangan dan operasional;
c) jika pemisahan secara fisik tidak dapat dilakukan, maka Bank harus memisahkan jaringan komunikasi secara *logic* dan memantau *security access* di jaringan

komunikasi;

d) keputusan untuk terhubung ke jaringan komunikasi di luar Bank harus sesuai dengan persyaratan pengamanan dan secara formal disetujui oleh manajemen sebelum pelaksanaan;

e) menerapkan pengendalian yang dapat membatasi *network traffic* yang tidak sah atau tidak diharapkan;

f) konfigurasi perangkat jaringan komunikasi harus diatur dengan baik. Fungsi-fungsi atau *services* yang tidak dibutuhkan harus dinonaktifkan;

g) penggunaan perangkat pengamanan jaringan komunikasi, seperti *firewall, Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS);

h) penggunaan penambahan perangkat monitor jaringan komunikasi (*network management system*) dengan memperhatikan pengamanannya; dan

i) pengujian secara berkala terhadap keamanan jaringan komunikasi, misalnya dengan *penetration testing*.

3) Pengoperasian dan Pemeliharaan Jaringan Komunikasi

Pengoperasian dan pemeliharaan jaringan komunikasi paling sedikit harus memperhatikan:

a) petugas yang mengoperasikan jaringan komunikasi harus secara jelas ditunjuk oleh manajemen, memiliki kemampuan pengetahuan dan keterampilan yang cukup, serta diberi tugas dan wewenang yang memadai untuk menjalankan fungsinya;

b) Bank harus memiliki *incident response plan* terhadap gangguan dan serangan jaringan komunikasi;

c) Bank harus memiliki fasilitas rekam cadang (*backup*) perangkat keras atau perangkat lunak jaringan komunikasi, termasuk mekanisme *restart/recovery* yang telah teruji. Fasilitas rekam cadang (*backup*) tersebut sebaiknya memiliki risiko yang berbeda dengan perangkat utama seperti menggunakan pihak penyedia jasa yang berbeda; dan

d) *patch* dan *release* harus selalu dikinikan setelah melalui pengujian intern untuk meyakini bahwa

kelemahan telah diperbaiki.

4) Dokumentasi

Untuk dapat mengendalikan kegiatan pengelolaan jaringan komunikasi, Bank harus memiliki dokumentasi jaringan komunikasi yang lengkap dan terkini, antara lain:

a) kebijakan, standar, prosedur, dan *baseline* tentang jaringan komunikasi;
b) diagram jaringan komunikasi secara rinci;
c) daftar dan spesifikasi perangkat lunak dan perangkat keras jaringan komunikasi;
d) daftar permasalahan dan penanganannya;
e) laporan pemantauan jaringan komunikasi;
f) laporan perencanaan kapasitas jaringan komunikasi;
g) perjanjian dan SLA dengan pihak penyedia jasa TI fasilitas jaringan komunikasi;
h) dokumen pengujian jaringan komunikasi;
i) dokumen pengimplementasian jaringan komunikasi;
j) dokumen perubahan jaringan komunikasi disertai alasan perubahan; dan
k) daftar pengguna dan wewenangnya.

4.3.2. Pemantauan Risiko

Pemantauan terhadap risiko yang mungkin timbul dalam jaringan komunikasi yang digunakan oleh Bank antara lain mencakup hal-hal:

a. jejak audit yang tersedia harus dipantau secara teratur untuk dapat mendeteksi secara dini ada tidaknya penyimpangan;
b. kinerja jaringan komunikasi diukur secara berkala berdasarkan tingkat ketersediaan (*availability*) dan *response time;*
c. Bank harus memantau kapasitas yang digunakan dan diperlukan untuk rencana pengembangan bisnis dibandingkan dengan kapasitas terpasang;
d. Bank harus memantau dan menindaklanjuti penyusupan atau serangan terhadap jaringan komunikasi; dan
e. Bank harus melakukan kaji ulang pemberian akses kepada pengguna secara berkala untuk meyakini bahwa akses yang diberikan masih sesuai dengan tugas dan wewenang. Selain itu, perlu dilakukan kaji ulang atas pengguna jaringan komunikasi

di Bank yang memiliki akses ke jaringan komunikasi di luar Bank.

BAB V PENGAMANAN INFORMASI

5.1. Pendahuluan

Informasi adalah aset yang sangat penting bagi Bank, baik informasi yang terkait dengan nasabah, keuangan, laporan, maupun informasi lainnya. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan, atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non-finansial 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 (misalnya sumber daya listrik, AC), dan SDM (termasuk kualifikasi dan keterampilan) namun juga informasi dalam bentuk yang lebih luas.

5.2. Kebijakan, Standar, dan Prosedur terkait Pengamanan Informasi

Sesuai Pasal 16 POJK MRTI, Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dengan memperhatikan paling sedikit:

a. pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) secara efektif dan efisien dengan memperhatikan kepatuhan terhadap ketentuan;
b. pengamanan informasi yang dilakukan terhadap aspek teknologi, SDM, dan proses dalam penggunaan TI;
c. pengamanan informasi yang diterapkan berdasarkan hasil penilaian terhadap risiko (*risk assessment*) pada informasi yang dimiliki Bank; dan
d. ketersediaan manajemen penanganan insiden dalam pengamanan informasi.

Selain kewajiban tersebut, 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.

Disamping itu, Bank perlu mempertimbangkan implementasi standar internasional di bidang pengamanan informasi seperti *International Organization for Standardization* (ISO), *International Electrotechnical Commission* (IEC), *Control Objective for Information and Related Technology* (COBIT), *Information Technology Infrastructure Library* (ITIL) dan standar nasional seperti Standar Nasional Indonesia (SNI), dengan memperhatikan tujuan, kebijakan usaha, ukuran, dan kompleksitas usaha Bank yang meliputi antara lain keragaman dalam jenis transaksi, produk, atau jasa dan jaringan kantor, serta teknologi pendukung yang digunakan.

5.2.1. Kebijakan Pengamanan Informasi

Manajemen Bank harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus sesuai dengan penerimaan risiko (*risk appetite*) dan dikomunikasikan secara berkala kepada seluruh pegawai Bank dan pihak ekstern yang terkait. Disamping itu, perlu dilakukan evaluasi kebijakan secara berkala dan apabila terdapat perubahan penting. Kebijakan tentang pengamanan informasi harus mencakup paling sedikit:

a. tujuan pengamanan informasi yang paling sedikit meliputi pengelolaan aset, SDM, pengamanan fisik, pengamanan *logic (logical security),* pengamanan operasional TI, penanganan insiden pengamanan informasi, dan pengamanan informasi dalam pengembangan sistem;
b. komitmen manajemen terhadap pengamanan informasi sejalan dengan strategi dan tujuan bisnis;
c. kerangka acuan dalam menetapkan pengendalian melalui pelaksanaan manajemen risiko Bank;
d. kepatuhan terhadap ketentuan intern dan ketentuan peraturan perundang-undangan antara lain Undang-Undang mengenai Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah mengenai Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE);
e. pelatihan dan peningkatan kesadaran atas pentingnya

pengamanan informasi (*security awareness program*);

f. analisis dampak pengamanan informasi terhadap kelangsungan bisnis;
g. tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi;
h. sanksi atas pelanggaran kebijakan pengamanan informasi; dan
i. dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

5.2.2. Standar Pengamanan Informasi

Manajemen Bank harus menetapkan standar pengamanan informasi sesuai dengan kebijakan pengamanan informasi dengan antara lain mengacu pada ketentuan peraturan perundang-undangan dan *best practice.* Standar tentang pengamanan informasi merupakan:

a. dasar untuk melaksanakan dan menilai kepatuhan pelaksanaan ketentuan terkait pengamanan informasi; dan
b. acuan untuk menyusun prosedur pengamanan informasi.

Contoh standar pengamanan informasi antara lain:

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.

5.2.3. Prosedur Pengamanan Informasi

5.2.3.1. Prosedur Pengelolaan Aset

Prosedur pengelolaan aset meliputi paling sedikit:

a. aset Bank yang terkait dengan informasi harus diidentifikasikan, ditentukan pemilik atau penanggungjawabnya, dan dicatat agar dapat dilindungi secara tepat;
b. aset yang terkait dengan informasi tersebut dapat berupa data (*hardcopy* atau *softcopy*), perangkat lunak, perangkat keras, jaringan, peralatan pendukung, misalnya sumber daya listrik dan AC, dan SDM termasuk kualifikasi dan keterampilan;
c. pengaturan penggunaan informasi dan aset harus

diidentifikasi, didokumentasikan, dan diimplementasikan. Seluruh pegawai Bank dan pihak ketiga harus mematuhi pengaturan tersebut seperti pengaturan penggunaan surat elektronik, *internet*, *mobile devices, teleworking,* dan lainnya; dan

d. informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya. Contoh dari klasifikasi tersebut adalah informasi ”rahasia” (misalnya data simpanan nasabah dan data pribadi nasabah), ”intern” (misalnya peraturan tentang gaji pegawai Bank), dan ”biasa” (misalnya informasi tentang produk perbankan yang ditawarkan kepada masyarakat). Klasifikasi dapat dibuat berdasarkan nilai, tingkat kerahasiaan, hukum atau ketentuan, dan tingkat kepentingan bagi Bank.

5.2.3.2. Prosedur Pengelolaan Sumber Daya Manusia

Prosedur pengelolaan SDM paling sedikit meliputi:

a. Bank harus menerapkan pengendalian yang memadai sebelum mempekerjakan pegawai TI (tetap, kontrak, atau honorer), konsultan, termasuk pegawai pihak penyedia jasa TI pada posisi yang memiliki kerentanan atau dampak yang besar terhadap pengamanan informasi. Sebagai contoh yaitu melakukan *background check* catatan kriminal atau kejahatan lainnya seperti pencurian data, dan lain-lain saat melakukan rekrutmen untuk posisi *network administrator* atau *system administrator*;

b. SDM baik pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi;

c. peran dan tanggung jawab SDM baik pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI 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 dengan pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI harus tercantum

ketentuan mengenai pengamanan TI yang sesuai dengan kebijakan pengamanan informasi Bank. Sebagai contoh adalah perlu adanya klausula yang menyatakan bahwa mereka harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi;

e. selain perjanjian antara Bank dengan perusahaan penyedia jasa TI, semua pegawai perusahaan penyedia jasa TI yang ditugaskan di Bank harus menandatangani suatu pernyataan menjaga kerahasiaan informasi (*non-disclosure statement*), termasuk kerahasiaan informasi untuk keperluan perlindungan data nasabah;

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

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 pihak penyedia jasa TI yang disebabkan karena perubahan tugas atau selesainya masa kerja atau perjanjian.

5.2.3.3. Prosedur Pengamanan Fisik dan Lingkungan

Prosedur pengamanan fisik dan lingkungan paling sedikit meliputi:

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 AC, sumber daya listrik, dan *fire alarm* harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;

d. aset milik pihak penyedia jasa TI 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.

5.2.3.4. Prosedur Pengendalian Akses

Prosedur pengendalian akses paling sedikit meliputi:

a. pengendalian akses fisik dan *logic*;

b. Bank harus menerapkan metode identifikasi dan otentikasi (*authentication*) sesuai analisis risiko. Metode otentikasi yang digunakan dapat berupa satu atau kombinasi dari "*what you know"* (antara lain PIN dan *password*)*, "what you have"* (antara lain *handphone,* kartu magnetis dengan *chip,* dan token)*, "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 intern maupun ekstern Bank, misalnya vendor atau pihak penyedia jasa TI;

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, misalnya melalui kertas karbon berlapis dua sehingga hanya diketahui oleh pihak yang berhak;
3) *password* atau PIN awal bersifat khusus (*unique*) untuk setiap *user* dan tidak mudah ditebak;
4) pemilik *user-id* terutama dari pegawai Bank, pegawai honorer, dan pegawai pihak penyedia jasa TI harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan *user-id* dan *password* atau PIN saat menerima *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 *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*), misalnya kata *'pass*', *'password*', 'adm', '123', atau kata umum di kamus;
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 lainnya yang dimiliki oleh Bank dapat membantu pelaksanaan pengamanan *password* atau PIN, sebagai contoh:

   1) memaksa pengguna untuk mengubah *password* atau PIN-nya 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 respon 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 sharing* harus menetapkan pembatasan akses paling sedikit melalui penggunaan *password* atau PIN dan pengaturan pihak yang berwenang melakukan akses.

5.2.3.5. Prosedur Pengamanan Operasional TI

Prosedur pengamanan operasional TI paling sedikit meliputi:

a. Bank harus memelihara catatan dari versi *anti virus* dan perangkat lunak yang digunakan dan melakukan pemantauan informasi secara rutin tentang *patch*, *upgrade*, atau

permasalahan lain yang sesuai dengan versi yang digunakan serta melakukan evaluasi, pengujian, dan instalasi hal tersebut;

b. 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;

c. 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;

d. Jejak audit atau *log* harus dilindungi terhadap gangguan dan akses tidak sah;

e. Penunjuk waktu dari seluruh sistem elektronik Bank harus disinkronisasikan dengan sumber penunjuk waktu akurat yang disepakati;

f. Bank harus melakukan kaji ulang secara berkala atas layanan operasional TI yang dilakukan oleh pihak penyedia jasa TI. Periode kaji ulang harus ditetapkan dalam perjanjian kerjasama antara Bank dan pihak penyedia jasa TI; dan

g. Bank harus menerapkan pengendalian media fisik dalam transit, untuk melindungi media terhadap akses yang tidak sah, penyalahgunaan, atau kerusakan selama transportasi diluar batas fisik Bank.

5.2.3.6. Prosedur Pemantauan Pengamanan Informasi

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

5.2.3.7. Prosedur Penanganan Insiden dalam Pengamanan Informasi

Hal-hal yang harus diperhatikan Bank dalam melakukan penanganan insiden dalam pengamanan informasi antara lain sebagai berikut.

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 pihak penyedia jasa TI 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 hal-hal terkait pelaporan insiden dalam pengamanan informasi sebagai berikut:

    1) unit kerja atau personel yang harus dihubungi apabila pegawai Bank, pegawai honorer, maupun pihak penyedia jasa TI 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 hal-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. Adapun contoh klasifikasi insiden adalah sebagai berikut:
      a) *Denial of Service* (DoS);
      b) akses fisik dan *logic* yang dilakukan oleh pihak yang tidak berwenang terhadap Sistem Elektronik;
      c) penyebaran *malicious code* (misalnya virus, *worms*, dan *trojan horse*);
      d) pelanggaran terhadap kebijakan pengamanan informasi dalam penggunaan *resource* TI oleh pegawai Bank, pegawai honorer, maupun penyedia jasa TI (misalnya penggunaan *email* kantor untuk tujuan *spamming*); dan
      e) metode verifikasi oleh TRIPI untuk meyakini bahwa laporan insiden dalam pengamanan informasi yang disampaikan oleh PoC adalah 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;
   4) 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*; dan

5) pengkinian 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 pihak penyedia

jasa TI yang melaporkan insiden atau *vulnerabilities* TI yang berisiko dieksploitasi dan mengancam pengamanan informasi, dalam rangka mendorong tercapainya pengamanan informasi yang kuat atau memadai.

5.3. Proses Manajemen Risiko terkait Pengamanan Informasi

5.3.1. Pengukuran Risiko Pengamanan Informasi

Bank melakukan pengukuran kecenderungan atau probabilitas terjadinya risiko terkait pengamanan informasi (ancaman mengeksploitasi kelemahan) atas setiap aset dan besarnya dampak kerugian akibat hilangnya kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dari aset yang mungkin terjadi untuk dapat mengetahui besarnya risiko potensial yang harus dihadapi.

Setiap satuan kerja di Bank harus dapat menentukan kemungkinan adanya ancaman (*threats*), serangan (*attacks*), dan kerawanan (*vulnerability)* dari setiap aset yang teridentifikasi serta digunakan masing-masing satuan kerja dan kemungkinan dampak kerugian hilangnya kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dari aset yang dimiliki.

Proses ini harus dilakukan Bank karena identifikasi dan pengukuran risiko dapat menunjukkan potensi kegagalan atau kelemahan proses pengamanan informasi yang dapat berpengaruh pada kesuksesan bisnis Bank sehingga Bank dapat melakukan penanganan yang tepat terhadap risiko potensial.

5.3.2. Pengendalian dan Mitigasi Risiko

Berdasarkan hasil pengukuran risiko, Bank harus menetapkan bentuk penanganan dan pengendalian risiko yang akan diterapkan untuk meminimalisasi risiko yang dihadapi Bank. Bank dapat menganalisis kelemahan dari bentuk pengendalian yang telah diterapkan dan bentuk pengendalian pengamanan yang dapat direkomendasikan untuk diterapkan kemudian.

Pengendalian intern juga dilakukan untuk memastikan bahwa pengendalian pengamanan informasi telah diterapkan, memadai, dan berjalan secara efektif sesuai dengan kebijakan, standar, dan prosedur pengamanan informasi yang berlaku. Evaluasi dan penyempurnaan terhadap kebijakan, standar, prosedur, dan sistem

pengamanan informasi harus selalu dilakukan secara terencana, antara lain dengan melaksanakan pemantauan terhadap:

a. perkembangan teknik atau metode baru yang mengancam sistem pengamanan informasi Bank;
b. laporan kinerja pengamanan informasi dalam rangka mengidentifikasi tren ancaman atau kelemahan pengendalian pengamanan;
c. tindak lanjut penanganan serangan atau insiden pengamanan informasi terhadap Bank; dan
d. efektivitas penerapan kebijakan, standar, prosedur, dan pengendalian pengamanan informasi.

BAB VI RENCANA PEMULIHAN BENCANA

6.1 Pendahuluan

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, huru-hara, dan sebagainya. 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 yaitu proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional Bank tetap dapat berfungsi walaupun terdapat gangguan atau bencana guna melindungi kepentingan para pemangku kepentingan. Rencana Pemulihan Bencana menekankan pada aspek teknologi dengan fokus pada pemulihan data (*data recovery* atau *restoration plan*) dan berfungsinya sistem aplikasi dan infrastruktur TI yang kritikal.

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

6.2.1. Kebijakan terkait Rencana Pemulihan Bencana

a. Penyusunan tim kerja Rencana Pemulihan Bencana

Bank harus memiliki kebijakan terkait Rencana Pemulihan Bencana yang mendukung efektivitas pelaksanaan Rencana Pemulihan Bencana pada saat diperlukan.

Bank perlu membentuk suatu organisasi atau tim kerja untuk mengoordinasikan pelaksanaan Rencana Pemulihan Bencana, yang terdiri atas:

1) koordinator;
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 meliputi:

i. bertanggung jawab penuh terhadap efektivitas pelaksanaan Rencana Pemulihan Bencana, termasuk memastikan bahwa program *awareness* atas Rencana Pemulihan Bencana diterapkan;
ii. memutuskan kondisi bencana dan pemulihannya;
iii. menentukan skenario pemulihan yang akan digunakan apabila terjadi gangguan atau bencana berdasarkan skala prioritas atas aktivitas, fungsi, dan jasa yang dianggap kritis;
iv. melakukan kaji ulang atas laporan mengenai setiap tahapan dalam pengujian dan pelaksanaan Rencana Pemulihan Bencana; dan
v. melaksanakan komunikasi kepada pihak intern dan ekstern Bank dalam hal terjadi gangguan operasional yang bersifat *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-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 merespon berbagai skenario ancaman dan gangguan serta bencana yang sifatnya tidak terduga yang bersumber dari kondisi intern dan/atau ekstern.
3) Rencana Pemulihan Bencana bersifat spesifik, terdapat kondisi-kondisi tertentu dan tindakan yang dibutuhkan segera untuk mengatasi kondisi tersebut.
4) Dilakukan pengujian dan pengkinian secara berkala atas Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
5) Rencana Pemulihan Bencana dan hasil pengujian Rencana

Pemulihan Bencana harus dikaji ulang secara berkala, paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

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

Efektifitas dari suatu Rencana Pemulihan Bencana bergantung pada kemampuan manajemen 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-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) tingkat ketergantungan terhadap pihak penyedia jasa baik TI maupun non TI;
3) jangka waktu Bank dapat beroperasi tanpa sistem atau fasilitas yang mengalami gangguan dan/atau toleransi jangka waktu pemulihan sistem atau fasilitas tersebut hingga dapat berfungsi kembali;
4) kebutuhan minimal jumlah personel, data, kelengkapan sistem, dan fasilitas yang diperlukan agar bisnis dapat beroperasi (*minimum resources requirement*);
5) dampak potensial dari kejadian yang bersifat tidak spesifik dan tidak dapat dikontrol terhadap proses bisnis dan pelayanan kepada nasabah;
6) dampak gangguan dan/atau bencana terhadap seluruh satuan kerja dan fungsi bisnis, bukan hanya terhadap *data processing;*
7) estimasi *downtime* maksimum yang dapat ditoleransi, tingkat toleransi atas kehilangan data dan terhentinya proses bisnis, dan dampak *downtime* terhadap kerugian finansial;
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* paling sedikit mencakup hal-hal:

1) melakukan analisis atas dampak gangguan atau bencana terhadap Bank, nasabah, dan industri keuangan;
2) melakukan *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) meyakini 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.

6.2.2. Prosedur terkait Rencana Pemulihan Bencana

a. Jenis Prosedur Rencana Pemulihan Bencana

Adapun jenis prosedur dalam Rencana Pemulihan Bencana antara lain mencakup:

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 paling sedikit mencakup 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 hal-hal yang berkaitan dengan *data files* dan *vital records* juga perlu diperhatikan seperti keberadaan Pusat Pemulihan Bencana dan 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 pihak penyedia jasa TI. Dalam penyelenggaraan Pusat Pemulihan Bencana, Bank harus memperhatikan hal-hal:

1) Pusat Pemulihan Bencana hendaknya ditempatkan pada lokasi yang terpisah dari lokasi Pusat Data, dengan memperhatikan faktor geografis:

a) jangkauan geografis atas suatu gangguan atau bencana dan dampaknya terhadap kota atau wilayah tempat lokasi Pusat Pemulihan Bencana berada; dan

b) analisis risiko yang berkaitan dengan lokasi Pusat Pemulihan Bencana (seperti tidak berlokasi di wilayah rawan gempa, banjir, atau petir) dan terhubung dengan infrastruktur komunikasi dan listrik yang

berbeda dengan Pusat Data, serta fasilitas lain yang diperlukan untuk tetap berjalannya suatu sistem;

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-hal yang harus diperhatikan dalam rekam cadang (*backup*) dokumentasi, sistem, dan data antara lain:

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 diperbaharui;
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 (*labeling*) 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*); dan

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

e. Fasilitas Komunikasi

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

6.3. 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 pihak penyedia jasa TI dalam kegiatan operasionalnya maka pengujian yang dilakukan juga perlu melibatkan pihak ekstern tersebut. Dalam hal Bank melakukan perubahan yang sangat mendasar terhadap sistem, aplikasi, atau infrastruktur TI Bank (misalnya perubahan pada *core banking system*) maka harus dilakukan pengujian Rencana Pemulihan Bencana paling lama 6 (enam) bulan setelah perubahan sistem dimaksud diimplementasikan.

6.3.1. Ruang Lingkup Pengujian Rencana Pemulihan Bencana

Manajemen harus secara jelas menentukan fungsi, sistem, dan proses yang akan diuji. Hal-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.

6.3.2. 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 mengenai:

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

6.3.3. 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 meliputi:

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 perubahannya; 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.

6.4. Pemeliharaan Rencana Pemulihan Bencana dan Audit Intern

6.4.1. 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*), meningkatkan pemahaman semua pihak di Bank maupun di penyedia jasa TI 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 pihak penyedia jasa TI.

Bank harus melakukan pengkinian Rencana Pemulihan Bencana untuk meyakinkan kesesuaiannya dengan kondisi ekstern maupun intern. Dalam melakukan pengkinian, hal-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 revisi tersebut harus didokumentasikan dan didistribusikan kepada satuan kerja TI.

6.4.2. 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 r*isk assessment*;
d. kecukupan prosedur pengujian Rencana Pemulihan Bencana;
e. efektifitas 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.

BAB VII LAYANAN PERBANKAN ELEKTRONIK

7.1. Pendahuluan

Perkembangan pesat TI mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik atau dikenal dengan Layanan Perbankan Elektronik. Contoh Layanan Perbankan Elektronik antara lain *Automated Teller Machine* (ATM), *Cash Deposit Machine* (CDM), *phone banking*, *Short Message Services* (SMS) *banking*, *Electronic Data Capture* (EDC), *Point of Sales* (POS), *internet banking*, dan *mobile banking*.

Penggunaan Layanan Perbankan Elektronik berpotensi meningkatkan risiko antara lain risiko operasional, risiko hukum, dan risiko reputasi. Oleh karena itu, penyediaan Layanan Perbankan Elektronik harus memperhatikan prinsip kehati-hatian, prinsip pengamanan, dan perlindungan nasabah yang memadai serta searah dengan strategi bisnis Bank.

7.2. Kebijakan, Standar, dan Prosedur terkait Layanan Perbankan Elektronik

Sesuai Pasal 28 POJK MRTI, permohonan persetujuan Layanan Perbankan Elektronik yang diajukan oleh Bank wajib dilengkapi bukti kesiapan untuk menyelenggarakan Layanan Perbankan Elektronik, antara lain kebijakan, sistem, prosedur, dan kewenangan dalam penerbitan produk Layanan Perbankan Elektronik. Hal-hal yang perlu diperhatikan antara lain sebagai berikut.

a. Kebijakan, sistem, dan prosedur secara tertulis untuk setiap Layanan Perbankan Elektronik yang diterbitkan paling sedikit memuat:
   1) kebijakan dan prosedur tertulis (*standard operating procedures)* produk dan aktivitas Layanan Perbankan Elektronik;
   2) tanggung jawab dan kewenangan dalam pengelolaan produk dan aktivitas Layanan Perbankan Elektronik;
   3) sistem informasi akuntansi produk dan aktivitas Layanan Perbankan Elektronik termasuk keterkaitan dengan sistem

informasi akuntansi Bank secara menyeluruh; dan

4) prosedur identifikasi, pengukuran, pemantauan, dan pengendalian berbagai risiko yang melekat pada produk dan aktivitas Layanan Perbankan Elektronik.

b. Setiap kebijakan, sistem, dan prosedur tertulis dimaksud harus memenuhi prinsip pengendalian pengamanan data nasabah dan transaksi Layanan Perbankan Elektronik, yaitu:

1) prinsip kerahasiaan (*confidentiality*)
Bank memastikan bahwa metode dan prosedur yang digunakan dapat melindungi kerahasiaan data nasabah;

2) prinsip integritas (*integrity*)
Bank memastikan bahwa metode dan prosedur yang digunakan mampu menjamin data yang digunakan akurat, andal, konsisten, dan terbukti kebenarannya sehingga terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan, dan perusakan data;

3) prinsip ketersediaan (*availability*)
Bank memastikan ketersediaan layanan dan Sistem Elektronik yang digunakan untuk menghasilkan data nasabah secara berkesinambungan;

4) prinsip keaslian (*authentication*)
Bank harus dapat menguji keaslian identitas nasabah untuk memastikan informasi yang disampaikan dan/atau transaksi keuangan dilakukan oleh nasabah yang berhak;

5) prinsip tidak dapat diingkari (*non repudiation*)
Bank harus menyusun, menetapkan, dan melaksanakan prosedur yang dapat memastikan bahwa transaksi yang telah dilakukan nasabah tidak dapat diingkari dan dapat dipertanggungjawabkan;

6) prinsip pengendalian otorisasi dalam sistem, Pangkalan Data (*Database*), dan aplikasi (*authorization of control*)
Bank memastikan antara lain:

a) adanya pengendalian terhadap hak akses dan otorisasi yang tepat terhadap sistem, Pangkalan Data (*Database*) dan aplikasi yang digunakan dalam penyelenggaraan TI; dan

b) seluruh informasi dan data penyelenggaraan TI yang bersifat rahasia hanya dapat diakses oleh pihak yang telah memiliki otorisasi serta harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi oleh pihak yang tidak berwenang;

7) prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*)

Bank memastikan terdapat pemisahan tugas dan tanggung jawab terkait sistem, Pangkalan Data (*Database*) dan aplikasi yang digunakan dalam penyelenggaraan TI untuk terlaksananya fungsi *check and balance*, misalnya terdapat pemisahan tugas antara pihak yang menginisiasi atau meng-*input* data dengan pihak yang bertanggung jawab untuk memverifikasi dan/atau mengotorisasi kebenaran data tersebut; dan

8) prinsip pemeliharaan jejak audit (*maintenance of audit trails*)

Bank memastikan ketersediaan dan pemeliharaan *log* transaksi sesuai dengan kebijakan retensi data dan ketentuan peraturan perundang-undangan, agar terdapat jejak audit yang jelas untuk membantu pembuktian, penyelesaian perselisihan, dan pendeteksian usaha penyusupan pada Sistem Elektronik. Bank harus menganalisis dan mengevaluasi fungsi jejak audit secara berkala.

Dalam menetapkan pengendalian pengamanan pada Layanan Perbankan Elektronik, Bank selain harus memperhatikan pengamanan layanan terhadap nasabah juga memperhatikan pengamanan serta hak dan kewajiban pihak lain yang terkait dan/atau yang bekerja sama dengan Bank dalam menyelenggarakan Layanan Perbankan Elektronik, khususnya terkait pengelolaan, penggunaan, dan penyimpanan data nasabah Layanan Perbankan Elektronik.

7.3. Manajemen Risiko Layanan Perbankan Elektronik

7.3.1. Pengukuran Risiko Terkait Layanan Perbankan Elektronik

Pengukuran dilakukan terhadap potensi kerugian yang terjadi (*loss*

event) pada setiap jenis Layanan Perbankan Elektronik. Untuk dapat memantau besar dan kecenderungan risiko dari setiap jenis Layanan Perbankan Elektronik maka Bank harus membuat Pangkalan Data (*Database*) yang berisi data historis kerugian (*loss event database)* setiap jenis Layanan Perbankan Elektronik. Jenis risiko terkait Layanan Perbankan Elektronik adalah sebagai berikut.

a. Risiko umum, antara lain:
   1) risiko operasional yaitu risiko yang timbul atau berasal dari *fraud*, kesalahan dalam proses, gangguan sistem atau kegiatan tidak terduga yang menyebabkan ketidakmampuan Bank untuk menyediakan produk atau layanan serta menimbulkan kerugian bagi Bank maupun nasabah. Risiko operasional juga dapat mencakup risiko terkait transaksi yang merupakan risiko yang dapat timbul dari kurang memadainya pelaksanaan prinsip pengendalian pengamanan;
   2) risiko kredit yaitu risiko yang timbul apabila Bank memberikan kredit melalui media elektronik misalnya produk kartu kredit;
   3) risiko hukum dan kepatuhan yang timbul dari:
      a) ketidakpatuhan terhadap hukum dan/atau peraturan dari otoritas pengawas;
      b) perbedaan dengan hukum di negara lain dalam hal *cross border transaction;*
      c) ketidakpatuhan terhadap ketentuan peraturan perundang-undangan mengenai kerahasiaan data nasabah dan ketentuan peraturan perundang-undangan mengenai transparansi informasi produk; dan
      d) keterbatasan ketentuan peraturan perundang-undangan sebagai dasar hukum transaksi Layanan Perbankan Elektronik;
   4) risiko stratejik merupakan risiko yang dapat timbul dari;
      a) ketidaksesuaian dengan tujuan atau rencana bisnis Bank;
      b) perencanaan investasi pada Layanan Perbankan Elektronik yang kurang memadai dapat menyebabkan

tidak optimalnya *return on investment* yang diperoleh dibandingkan dengan biaya yang dikeluarkan; dan

c) pengelolaan hubungan (*relationship management*) dengan pihak penyedia jasa TI yang kurang optimal;

5) risiko reputasi yaitu risiko yang timbul dari kemungkinan menurunnya atau hilangnya kepercayaan nasabah karena s*ervice level delivery* kepada nasabah tidak terjaga seperti kelambatan atau tidak tersedianya Layanan Perbankan Elektronik, kelambatan respon atas komplain nasabah, ketidakamanan sistem, dan adanya gangguan pada sistem;

6) risiko pasar yaitu risiko yang timbul dalam hal Bank membuat produk yang memiliki fitur yang memungkinkan eksekusi transaksi yang terpapar perubahan tingkat bunga, perubahan nilai tukar misalnya pada layanan transfer di *internet banking* dari rekening rupiah milik nasabah ke rekening valas tujuan di luar negeri; dan

7) risiko likuiditas yaitu risiko yang timbul dalam hal Bank tidak membatasi jumlah yang dapat ditransfer oleh nasabah korporasi melalui *internet banking*.

b. Risiko spesifik, antara lain:

1) risiko operasional yang mungkin timbul dari transaksi Layanan Perbankan Elektronik diantaranya adalah kecurangan, penyadapan, kesalahan, kerusakan, atau tidak berfungsinya sistem;

2) risiko yang mungkin timbul dari transaksi Layanan Perbankan Elektronik lintas negara antara lain risiko hukum mengingat transaksi melewati batas wilayah hukum yang berbeda. Risiko ini timbul karena terdapat perbedaan ketentuan peraturan perundang-perundangan di antara kedua wilayah hukum, seperti perlindungan konsumen, kerahasiaan Bank dan data pribadi nasabah, persyaratan pelaporan, dan anti pencucian uang dan pencegahan pendanaan terorisme;

3) risiko dalam penyelenggaraan *internet banking* meliputi:

a) nasabah memperoleh informasi yang salah atau tidak akurat melalui internet;

b) pencurian data finansial dari Pangkalan Data (*Database*) Bank melalui *informational and communicative internet banking* yang tidak terisolasi;

c) terdapat ancaman atau serangan misalnya *defacing*, *cybersquating, denial of service*, pemutusan jaringan (*network interception*), *man-in-the middle-attack*, dan virus;

d) terjadi pencurian identitas (*identity theft)* misalnya *phising, key logger, spoofing,* dan *cybersquating*; dan

e) terjadi transaksi yang dilakukan oleh pihak yang tidak berwenang (*unauthorized transaction*) atau terjadi *fraud*;

4) ancaman keamanan pada produk yang menggunakan teknologi *wireless* misalnya *mobile banking* antara lain penyadapan komunikasi akibat belum semua transaksi melalui *mobile banking* dienkripsi, *denial of service attack*, virus, *worm, trojan*, dan penggandaan *sim card*; dan

5) ancaman keamanan pada produk *phone banking* yang rentan terhadap penyadapan.

7.3.2. Pengendalian Risiko terkait Layanan Perbankan Elektronik

Dalam rangka pengendalian risiko, Bank harus melakukan mitigasi atas risiko umum dan risiko spesifik yang mungkin terjadi dalam Layanan Perbankan Elektronik dengan memperhatikan prinsip pengendalian pengamanan data nasabah dan transaksi Layanan Perbankan Elektronik, antara lain dengan:

a. melakukan langkah-langkah yang memadai untuk menguji keaslian (*authentication*) identitas dan kewenangan (*authorization*) nasabah yang melakukan transaksi melalui Layanan Perbankan Elektronik;

b. memiliki kebijakan dan prosedur tertulis untuk memastikan bahwa Bank mampu menguji keaslian identitas dan kewenangan nasabah;

c. menggunakan berbagai metode untuk menguji keaslian yang didasarkan atas penilaian manajemen risiko Layanan Perbankan Elektronik, sensitivitas, dan nilai data yang disimpan. Dalam menggunakan metode pengujian keaslian,

Bank memperhatikan hal-hal sebagai berikut:

1) menerapkan kombinasi paling sedikit 2 (dua) faktor otentikasi (*two factor authentication*) yaitu "*what you know*" (seperti PIN atau *password*), *"what you have"* (seperti identitas elektronik, kartu magnetis dengan *chip,* token, atau *digital signature*), dan/atau *"something you are"* (antara lain *biometric* seperti retina atau sidik jari);
2) persyaratan jumlah karakter minimum PIN. Khusus untuk PIN yang digunakan dalam alat pembayaran dengan menggunakan kartu, *mobile banking,* dan *internet banking*, panjang PIN harus paling sedikit terdiri dari 6 (enam) digit karakter;
3) adanya batasan maksimum kesalahan memasukkan PIN untuk menghambat upaya akses secara tidak sah;
4) Bank harus memastikan penerapan prinsip kehati-hatian dalam penggunaan metode pengujian keaslian yang meliputi:
    a) pembuatan, validasi, dan enkripsi PIN dan metode pengujian keaslian lainnya harus menggunakan metode yang diyakini keamanannya. Khusus untuk metode enkripsi yang digunakan pada alat pembayaran menggunakan kartu, metode enkripsi PIN harus paling sedikit menggunakan metode *triple Data Encryption Standard* (*triple* DES) berdasarkan standar kartu dan/atau *chip* yang memenuhi standar;
    b) Pangkalan Data (*Database*) pengujian keaslian yang menyediakan akses kepada rekening nasabah pada Layanan Perbankan Elektronik dilindungi dari gangguan dan perusakan;
    c) setiap penambahan, penghapusan, atau perubahan Pangkalan Data (*Database*) dan pengujian keaslian telah diotorisasi dengan tepat oleh pihak yang berwenang;
    d) khusus untuk Layanan Perbankan Elektronik dengan menggunakan kartu, fungsi pembuatan dan pengiriman PIN harus terpisah dari fungsi pembuatan dan pengiriman kartu;

e) khusus untuk Layanan Perbankan Elektronik dengan menggunakan kartu, fungsionalitas dan keamanan kartu harus diuji menggunakan standar kartu dan *chip* yang memenuhi standar;

f) terdapat sarana pengendalian yang tepat terhadap sistem Layanan Perbankan Elektronik sehingga pihak ketiga yang tidak dikenal tidak dapat menggantikan nasabah yang telah dikenal; dan

g) terdapat kebijakan yang menyatakan bahwa jika terdapat indikasi telah terjadi pencurian data yang terkait dengan aspek otentikasi nasabah maka Bank harus melakukan penggantian data otentikasi nasabah dimaksud secepatnya;

5) Bank harus menyusun dan menetapkan prosedur untuk menjamin bahwa transaksi tidak dapat diingkari oleh nasabah (*non repudiation*) sehingga transaksi dapat dipertanggungjawabkan, yang meliputi antara lain:

a) sistem Layanan Perbankan Elektronik telah dirancang untuk menghilangkan kemungkinan dilakukannya transaksi secara tidak sengaja oleh para pengguna yang berhak;

b) seluruh pihak yang melakukan transaksi telah diuji keasliannya;

c) data transaksi keuangan dilindungi dari kemungkinan pengubahan dan setiap pengubahan dapat dideteksi. Proses pencatatan transaksi keuangan harus dirancang sebaik mungkin agar dapat mencegah upaya pengubahan tidak sah. Setiap upaya pengubahan yang tidak sah perlu dicatat dan menjadi perhatian manajemen Bank; dan

d) penerapan metode untuk menjamin dipenuhinya prinsip tidak dapat diingkari (*non repudiation*), misalnya *digital signature* dan *Public Key Infrastructure* (PKI). Kunci-kunci (*keys*) yang digunakan untuk keperluan enkripsi harus dipelihara secara aman sehingga tidak ada yang mengetahui kombinasi kunci-kunci tersebut secara utuh;

d. memastikan terdapat pemisahan tugas dan tanggung jawab terkait penggunaan sistem, Pangkalan Data (*Database*), dan aplikasi Layanan Perbankan Elektronik. Bank harus memastikan terdapat *dual control* dan pemisahan tugas untuk memastikan terlaksananya fungsi *check and balance.* Bank perlu memastikan terdapat pemisahan tugas antara pihak yang menginisiasi atau meng-*input* data dan pihak yang bertanggung jawab untuk memverifikasi kebenaran data tersebut. Misalnya dalam suatu aplikasi perbankan, setiap penambahan atau perubahan Pangkalan Data (*Database*) yang dilakukan oleh *data entry* operator, akan efektif sepanjang disetujui oleh penyelia;

e. memastikan adanya pengendalian terhadap otorisasi dan hak akses (*privileges*) yang tepat terhadap sistem, Pangkalan Data (*Database*), dan aplikasi Layanan Perbankan Elektronik.

   Seluruh arsip dan data Bank yang bersifat rahasia hanya dapat diakses oleh pihak yang telah memiliki kewenangan dan otorisasi. Data Bank yang bersifat rahasia harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi oleh pihak yang tidak berwenang;

f. memastikan metode dan prosedur diterapkan untuk melindungi integritas data, catatan, dan informasi terkait transaksi Layanan Perbankan Elektronik dengan memperhatikan hal-hal sebagai berikut:

   1) Bank harus menerapkan metode dan teknik yang tepat untuk mengurangi ancaman ekstern seperti serangan virus dan *malicious transaction,* yang meliputi:

      a) perangkat lunak – penyediaan *virus scanning* dan anti virus untuk seluruh *entry point* dan masing-masing komputer;

      b) perangkat lunak untuk mendeteksi adanya penyusupan (*intrusion detection system*); dan

      c) pengujian penetrasi (*penetration testing*) terhadap jaringan intern dan ekstern secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun;

   2) Bank harus melakukan pengujian integritas data transaksi Layanan Perbankan Elektronik; dan

3) Bank harus melakukan pengendalian untuk memastikan seluruh transaksi telah dilaksanakan dengan benar;

g. memastikan tersedianya mekanisme penelusuran (*audit trail*) yang jelas untuk seluruh transaksi Layanan Perbankan Elektronik, yang mencakup hal-hal sebagai berikut:

1) Bank harus memelihara *log* transaksi berdasarkan kebijakan retensi data Bank sesuai ketentuan peraturan perundang-undangan guna tersedianya jejak audit yang jelas serta membantu penyelesaian perselisihan. Data transaksi yang diperlukan mencakup paling sedikit data nasabah, nomor rekening, jenis, waktu, lokasi, dan jumlah transaksi;

2) Bank harus memberikan notifikasi kepada nasabah apabila suatu transaksi telah berhasil dilakukan. Apabila terdapat transaksi yang ditolak maka perlu didokumentasikan dan terdapat prosedur tindak lanjutnya; dan

3) Bank harus memastikan tersedianya fungsi jejak audit untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan yang harus dikaji ulang atau dievaluasi secara berkala. Apabila sistem pemrosesan dan jejak audit merupakan tanggung jawab pihak ketiga maka proses jejak audit tersebut harus sesuai dengan standar yang ditetapkan oleh Bank. Bank harus memiliki kewenangan yang cukup untuk dapat mengakses jejak audit yang dipelihara oleh pihak ketiga tersebut;

h. melakukan pendeteksian dan pemantauan atas transaksi yang tidak sah atau tidak wajar misalnya melalui *Intrusion Detection System* (IDS) dan *fraud detection.* Selanjutnya Bank harus memiliki prosedur penanganan masalah atau kejahatan yang terdeteksi;

i. menerapkan langkah-langkah untuk melindungi kerahasiaan informasi Layanan Perbankan Elektronik. Prosedur pengamanan disesuaikan dengan tingkat sensitivitas informasi;

j. memiliki standar dan pengendalian atas penggunaan dan perlindungan data apabila pihak penyedia jasa TI memiliki akses terhadap data tersebut;

k. memiliki Rencana Pemulihan Bencana termasuk *contingency plan* yang efektif untuk memastikan tersedianya sistem dan jasa Layanan Perbankan Elektronik secara berkesinambungan; dan

l. mengembangkan rencana penanganan kejadian (*incident response plan*) yang cepat dan tepat untuk mengelola, mengatasi, dan meminimalisasi dampak suatu insiden, *fraud*, kegagalan sistem (intern dan ekstern), yang dapat menghambat penyediaan sistem dan jasa Layanan Perbankan Elektronik.

7.3.2.1. Pengendalian Risiko untuk Layanan Perbankan Elektronik Tertentu

a. Dalam menyediakan Layanan Perbankan Elektronik misalnya pada ATM dan *internet banking*, Bank juga harus memperhatikan kenyamanan dan kemudahan nasabah menggunakan fasilitas, termasuk efektivitas menu tampilan Layanan Perbankan Elektronik, khususnya dalam melakukan pilihan pesan yang diinginkan nasabah agar tidak terjadi kesalahan dan kerugian dalam transaksi.

   Dalam rangka meningkatkan pengamanan, Bank dapat menetapkan persyaratan atau melakukan pembatasan transaksi melalui Layanan Perbankan Elektronik untuk menjamin keamanan dan keandalan transaksi, misalnya meminta nasabah melakukan registrasi rekening pihak ketiga yang merupakan tujuan transfer dalam *mobile banking* atau membatasi nominal jumlah transaksi melalui ATM dan *internet banking*.

b. Dalam penyelenggaraan Layanan Perbankan Elektronik yang menyediakan sarana fisik seperti ATM, Bank harus melakukan pengendalian pengamanan fisik terhadap peralatan dan ruangan yang digunakan terhadap bahaya pencurian, perusakan, dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Bank harus melakukan pemantauan secara rutin untuk menjamin keamanan dan kenyamanan bagi nasabah pengguna Layanan Perbankan Elektronik.

c. Bank harus memastikan terdapatnya pengamanan atas aspek transmisi data antara terminal *Electronic Fund Transfer* (EFT) dengan *host computer*, terhadap risiko kesalahan transmisi,

gangguan jaringan, akses oleh pihak yang tidak bertanggung jawab, dan lain-lain. Pengamanan mencakup pengendalian terhadap peralatan yang digunakan, pemantauan terhadap akses perangkat lunak *Controller* (*Host-Front End*), pemantauan kualitas dan akurasi kinerja perangkat jaringan serta saluran transmisi.

d. *Point of Sales* (POS) atau *Electronic Data Capture* (EDC) memungkinkan transfer dana secara elektronik dari rekening nasabah kepada rekening *acquirer* atau *merchant* untuk pembayaran suatu transaksi. Transaksi dilakukan melalui POS Terminal yang berlokasi di pusat perbelanjaan atau pasar swalayan umumnya menggunakan suatu alat pembayaran dengan menggunakan kartu. Penyediaan POS dapat dilakukan sendiri oleh Bank penerbit maupun oleh *financial acquirer, technical acquirer,* dan perusahaan *switching.* Pihak penyedia POS Terminal harus selalu melakukan peningkatan pengamanan fisik di sekitar lokasi POS Terminal dan terhadap POS Terminal, antara lain dengan menggunakan POS Terminal yang dapat meminimalisasi kemungkinan adanya penyadapan baik di POS Terminal sendiri maupun dalam jaringan komunikasi.

e. Bagi Bank yang menyediakan jasa *mobile banking* maka Bank harus memastikan keamanan transaksi antara lain:
   1) menggunakan suatu *SIM Toolkit* dengan fitur enkripsi *end-to-end* dari *handphone* hingga *server mobile banking*, untuk melindungi pengiriman data pada *mobile banking*; dan
   2) melakukan *mutual authentication* yaitu pihak Bank dan nasabah dapat melakukan proses otentifikasi dengan *digital certificate* atau *personal authentication message* yaitu untuk membantu nasabah memastikan bahwa pihak yang bertransaksi dengan nasabah adalah pihak yang benar.

f. Dalam penyediaan jasa TI layanan *phone banking*, Bank harus memastikan keamanan transaksi diantaranya melalui hal-hal:
   1) layanan tidak digunakan untuk transaksi dengan nilai maupun risiko yang tinggi;

2) semua percakapan melalui *Interactive Voice Response* (IVR) direkam termasuk nomor telepon nasabah, detil transaksi, dan lain-lain;
3) layanan menggunakan metode otentifikasi yang andal dan aman; dan
4) penggunaan metode otentifikasi nasabah seperti PIN dan *password* untuk transaksi finansial.

7.3.2.2. Pengendalian Risiko terkait Layanan Perbankan Elektronik Lintas Negara

Dalam menyelenggarakan Layanan Perbankan Elektronik lintas negara (*cross border*), Bank antara lain perlu memperhatikan:

a. pembangunan program manajemen risiko yang efektif untuk aktivitas Layanan Perbankan Elektronik lintas negara (*cross border*). Sebelum Bank mengenalkan produk dan jasa Layanan Perbankan Elektronik lintas negara (*cross border*), manajemen Bank sebaiknya melakukan penilaian risiko dan *due diligence* yang tepat guna menjamin bahwa Bank secara tepat mengelola risiko-risiko yang ada. Selain memperhatikan aspek hukum dan ketentuan peraturan perundang-undangan di Indonesia, Bank perlu memperhatikan aspek hukum dan peraturan di negara tempat Bank akan menawarkan jasa Layanan Perbankan Elektronik lintas negara (*cross border*); dan
b. adanya pengungkapan yang cukup pada *website* atau informasi lainnya yang memungkinkan calon nasabah mengetahui identitas Bank, *home country*, otoritas pengawas Bank, dan izin yang diperoleh Bank, sebelum melakukan hubungan bisnis dengan Bank.

7.3.2.3. Pengendalian Risiko terkait Layanan Perbankan Elektronik yang Diselenggarakan oleh Pihak Penyedia Jasa TI

Dalam hal sistem penyelenggaraan Layanan Perbankan Elektronik dilakukan oleh pihak penyedia jasa TI misalnya perusahaan *switching* dan *Internet Service Provider* (ISP), Bank harus menetapkan dan menerapkan prosedur pengawasan dan *due diligence* yang menyeluruh dan berkelanjutan untuk mengelola hubungan Bank dengan pihak penyedia jasa TI tersebut. Untuk itu Bank harus membuat suatu perjanjian tertulis dengan pihak

penyedia jasa TI terkait Layanan Perbankan Elektronik yang secara rinci mengatur hak dan kewajiban, aspek pengamanan, dan melakukan pemantauan kinerja pihak penyedia jasa TI sesuai SLA.

7.4. Rencana Penerbitan Layanan Perbankan Elektronik Baru

Yang dimaksud dengan "produk Layanan Perbankan Elektronik baru" adalah produk baru yang karakteristiknya berbeda dengan produk yang telah ada di Bank dan/atau menambah atau meningkatkan eksposur risiko tertentu pada Bank, seperti *internet banking* dan *mobile banking* untuk nasabah penyimpan.

Dengan demikian jika Bank hanya menambah jenis layanan pada produk Layanan Perbankan Elektronik yang telah ada dan penambahan risikonya tidak signifikan, misalnya penambahan fasilitas pembayaran melalui Layanan Perbankan Elektronik yang semula hanya melayani pembayaran kartu kredit menjadi pembayaran listrik atau telepon maka penambahan layanan pembayaran tersebut tidak tergolong produk baru sehingga tidak perlu dilaporkan.

Namun jika Bank menambah layanan misalnya yang semula hanya menangani transaksi rupiah kemudian menambah layanan berupa transaksi valuta asing maka Bank harus melaporkan produk baru tersebut karena berdasarkan analisis risiko, transaksi tersebut dapat meningkatkan risiko pasar, risiko hukum, dan risiko lainnya.

Dalam hal TI yang digunakan dalam menyelenggarakan Layanan Perbankan Elektronik dilakukan oleh pihak penyedia jasa TI maka berlaku pula ketentuan penggunaan pihak penyedia jasa TI.

7.5. Permohonan Persetujuan terkait Layanan Perbankan Elektronik

Permohonan persetujuan penerbitan Layanan Perbankan Elektronik tidak berlaku untuk produk Layanan Perbankan Elektronik yang diatur secara khusus dalam ketentuan mengenai persyaratan persetujuan produk tersebut.

Selain bukti kesiapan dan dokumen pendukung untuk menyelenggarakan Layanan Perbankan Elektronik sebagaimana diatur dalam Pasal 28 POJK MRTI, Bank juga wajib melengkapi permohonan persetujuan Layanan Perbankan Elektronik dengan hasil analisis bisnis mengenai proyeksi produk baru 1 (satu) tahun yang akan datang, paling sedikit memuat:

a. potensi pasar yang ada;
b. segmen pasar yang akan dituju;
c. analisis persaingan usaha;
d. target nasabah yang ingin dicapai;
e. rencana kerja sama dengan pihak lain; dan
f. target pendapatan yang akan dicapai.

7.6. Realisasi Layanan Perbankan Elektronik

7.6.1. Pemeriksaan oleh Pihak Independen

Laporan realisasi Layanan Perbankan Elektronik harus dilengkapi dengan kajian pascaimplementasi (*postimplementation review*) oleh pihak independen. Pihak independen adalah pihak yang tidak terlibat dalam perancangan dan pengembangan sistem aplikasi, serta pengambilan keputusan untuk implementasi.

Hasil pemeriksaan oleh pihak independen ditujukan untuk memberikan pendapat atas karakteristik produk dan kecukupan pengamanan sistem TI terkait produk tersebut serta kepatuhan terhadap ketentuan peraturan perundang-undangan dan/atau *best practices* yang memenuhi standar internasional seperti ISO, IEC, COBIT, dan ITIL.

Hasil pemeriksaan dari pihak independen di luar Bank seperti kantor akuntan publik atau perusahaan konsultan di bidang *information technology security* diperlukan untuk produk Layanan Perbankan Elektronik yang baru pertama kali diterbitkan oleh Bank seperti *internet banking* yang bersifat transaksional dan *SMS banking* yang bersifat transaksional. Sedangkan untuk penambahan fitur produk Layanan Perbankan Elektronik yang telah ada di Bank, yang dapat menambah atau meningkatkan eksposur risiko Bank, dapat menggunakan pihak intern untuk melakukan kaji ulang independen (*independent review*).

Contoh:

a. penambahan fitur transaksi pemindahbukuan antar rekening melalui ATM yang sebelumnya tidak dapat dilakukan oleh nasabah;
b. penambahan fitur transaksi transfer antar Bank melalui ATM yang sebelumnya tidak dapat dilakukan oleh nasabah.

Bank perlu memastikan bahwa pihak ekstern memiliki kompetensi

dan pemahaman terhadap produk yang akan dikaji ulang terutama dalam aspek pengamanan TI. Dalam hal Bank menggunakan pihak intern untuk melakukan kaji ulang independen (*independent review*) maka Bank harus menyampaikan uraian tugas dan tanggung jawab pihak tersebut serta kedudukannya dalam struktur organisasi pada proyek pengembangan Layanan Perbankan Elektronik.

7.6.2. Ruang Lingkup Pemeriksaan Pihak Independen

Bank harus memastikan bahwa laporan yang disampaikan oleh pihak independen mengenai kesiapan TI Bank untuk kegiatan Layanan Perbankan Elektronik yang direncanakan memuat periode pemeriksaan, ruang lingkup, metode pemeriksaan, temuan, rekomendasi, tanggapan manajemen atas temuan, serta target penyelesaian. Adapun ruang lingkup pemeriksaan meliputi:

a. pengawasan aktif manajemen;
b. kecukupan kebijakan dan prosedur pengamanan sistem Layanan Perbankan Elektronik untuk memastikan terpenuhinya prinsip kerahasiaan, integritas, ketersediaan, dan tidak dapat diingkari dalam setiap transaksi Layanan Perbankan Elektronik;
c. kecukupan penerapan dan pemantauan terhadap pengamanan sistem Layanan Perbankan Elektronik yang disiapkan Bank meliputi:
    1) penerapan pengamanan sistem, infrastruktur (*server, firewall,* dan *router*), serta jaringan sistem Layanan Perbankan Elektronik;
    2) pengamanan untuk mendeteksi transaksi yang tidak wajar;
    3) terdapat pemeliharaan dan kaji ulang atas jejak audit *log* transaksi;
    4) pengamanan fisik yang memadai atas perangkat komputer dan perangkat komunikasi terkait Layanan Perbankan Elektronik;
    5) pengamanan atas jaringan intern Bank sehingga terlindung dari serangan yang berasal dari ekstern; dan
    6) pengamanan atas data dan Pangkalan Data (*Database*) transaksi Layanan Perbankan Elektronik;

d. penanganan terhadap kondisi tertentu, antara lain *fraud*;
e. Rencana Pemulihan Bencana dan prosedur tanggap darurat *(incident response management)*;
f. penggunaan pihak penyedia jasa TI sebagai penyelenggara Layanan Perbankan Elektronik;
g. kaji ulang atas analisis risiko produk baru Layanan Perbankan Elektronik yang meliputi paling sedikit risiko stratejik, risiko pengamanan, risiko hukum, dan risiko reputasi; dan
h. program edukasi dan perlindungan nasabah termasuk kehati-hatian dalam pembukaan rekening dan dalam melakukan transaksi melalui Layanan Perbankan Elektronik.

BAB VIII AUDIT INTERN TI

8.1. Pendahuluan

Sistem Pengendalian Intern (SPI) yang efektif merupakan komponen penting dalam manajemen Bank dan menjadi dasar bagi kegiatan operasional Bank yang sehat dan aman. SPI yang efektif antara lain dapat membantu manajemen 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. Audit intern TI sebagai salah satu bagian dari SPI diperlukan untuk melakukan evaluasi terhadap penyelenggaraan TI secara independen dan objektif untuk meningkatkan efisiensi dan efektivitas manajemen risiko, pengendalian intern, dan tata kelola yang baik. Audit TI yang dimaksud antara lain audit terhadap Pusat Data, Pusat Pemulihan Bencana, aplikasi, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi.

8.2. Kebijakan, Standar, dan Prosedur terkait Audit TI

Sesuai Pasal 18 POJK MRTI, pelaksanaan fungsi audit intern TI memperhatikan kepatuhan terhadap ketentuan mengenai standar pelaksanaan fungsi audit intern.

Dalam rangka 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 dan penggunaan 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 paling sedikit mencakup:
    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-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) pelanggaran terhadap kebijakan audit TI; dan
9) kaji ulang secara berkala paling sedikit 1 (satu) kali dalam 3 (tiga) tahun atas fungsi audit TI sebagai bagian dari fungsi audit intern secara keseluruhan oleh pihak independen.

b. Bank harus memiliki standar audit TI yang paling sedikit mencakup:
   1) Rencana Kerja Audit (*Audit Working Plan*/AWP);
   2) kertas kerja audit termasuk hasil atau temuan audit;
   3) Laporan Hasil Audit (LHA); dan
   4) pemantauan tindak lanjut hasil audit.

c. Bank harus memiliki prosedur audit TI yang paling sedikit mencakup:
   1) manajemen;
   2) pengembangan dan pengadaan;
   3) operasional TI;
   4) jaringan komunikasi;
   5) pengamanan informasi;
   6) Rencana Pemulihan Bencana;
   7) Layanan Perbankan Elektronik;
   8) penggunaan pihak penyedia jasa TI;

9) penyediaan jasa TI oleh Bank; dan
10) aplikasi bisnis seperti *core banking system*, kartu kredit, *treasury*, *remittance,* dan pembiayaan perdagangan (*trade finance*).

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

8.3. Proses Audit TI

a. Perencanaan Audit TI

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

1) mengidentifikasi aset TI yang berupa data, aplikasi, sistem operasi, teknologi, fasilitas, dan personel;
2) mengidentifikasi kegiatan dan proses bisnis yang menggunakan TI; dan
3) mengidentifikasi tingkat dampak risiko TI dalam operasional Bank dan mempertimbangkan skala prioritas berdasarkan tingkat risiko.

Rencana audit TI harus mendapat persetujuan dari presiden direktur atau direktur utama.

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 paling sedikit mencakup:

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 yang diperolehnya. 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 kode etik (etika) dalam melaksanakan tugas, yaitu 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 apapun 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 yang diperoleh dalam pelaksanaan tugas audit;

dan

2) tidak menggunakan data atau informasi yang diperoleh 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.

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

Sesuai Pasal 30 POJK MRTI, Bank wajib melaporkan hasil audit TI paling lambat 2 (dua) bulan setelah audit selesai dilakukan. LHA TI disusun berdasarkan format standar laporan. Laporan tersebut merupakan sarana bagi manajemen untuk membantu melakukan penilaian kualitas pengendalian TI. LHA TI harus disampaikan kepada satuan kerja yang diperiksa. Disamping itu, laporan tersebut disampaikan secara tepat waktu kepada direktur utama dan Dewan Komisaris atau komite audit dengan tembusan kepada direktur yang membawahkan fungsi kepatuhan. Pokok-pokok hasil audit TI disampaikan juga kepada Otoritas Jasa Keuangan.

d. Pemantauan Tindak Lanjut

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 tindak lanjut hasil pemeriksaan

disampaikan kepada direktur utama dan Dewan Komisaris atau komite audit dengan tembusan kepada direktur yang membawahkan fungsi kepatuhan.

Perubahan atas rencana dan realisasi tindak lanjut, serta target penyelesaian tindak lanjut harus disampaikan kepada auditor TI dan disetujui oleh direktur utama dan Dewan Komisaris atau komite audit dengan tembusan kepada direktur yang membawahkan fungsi kepatuhan.

8.4. Pemenuhan Fungsi Audit Intern TI

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. Disamping 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.

BAB IX PENGGUNAAN PIHAK PENYEDIA JASA TI

9.1 Pendahuluan

Dalam rangka meningkatkan efektivitas dan efisiensi pencapaian tujuan strategis, Bank dimungkinkan menggunakan pihak penyedia jasa TI. Hal ini sesuai dengan Pasal 20 POJK MRTI yang mengatur bahwa penyelenggaraan TI dapat dilakukan oleh Bank sendiri dan/atau pihak penyedia jasa TI. Yang dimaksud dengan menggunakan pihak penyedia jasa TI adalah penggunaan jasa pihak lain dalam menyelenggarakan kegiatan TI yang dapat menyebabkan Bank memiliki ketergantungan terhadap jasa yang diberikan secara berkesinambungan atau dalam periode tertentu.

Penggunaan pihak penyedia jasa TI dapat mempengaruhi risiko Bank antara lain risiko operasional, kepatuhan, hukum, dan reputasi. Risiko-risiko ini dapat timbul antara lain karena adanya kegagalan penyedia jasa TI dalam menyediakan jasa, pelanggaran hukum, atau ketidakmampuan untuk mematuhi hukum dan ketentuan peraturan perundang-undangan.

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

9.2. Kebijakan, Standar, dan Prosedur Penggunaan Penyedia Jasa TI

Dalam hal penyelenggaraan TI Bank dilakukan oleh pihak penyedia jasa TI, Bank harus memenuhi ketentuan sebagaimana diatur dalam Pasal 20 POJK MRTI, serta memiliki kebijakan, standar, dan prosedur penggunaan penyedia jasa TI.

9.2.1. Kebijakan Penggunaan Penyedia Jasa TI

Bank harus memiliki kebijakan mengenai penyelenggaraan TI kepada pihak lain yang paling sedikit mengatur mengenai:

a. Prinsip-prinsip penggunaan penyedia jasa TI
    1) Bank tetap bertanggung jawab terhadap layanan TI yang diselenggarakan oleh pihak penyedia jasa TI;
    2) penggunaan penyedia jasa TI tidak menghambat proses pengawasan oleh Otoritas Jasa Keuangan;
    3) keputusan penggunaan penyedia jasa TI harus sejalan

dengan rencana strategis TI Bank;

4) setiap penggunaan penyedia jasa TI harus dituangkan dalam perjanjian tertulis;
5) penggunaan penyedia jasa TI harus memberikan manfaat lebih besar dibandingkan dengan biaya yang dikeluarkan Bank; dan
6) penggunaan penyedia jasa TI harus didasarkan pada hubungan kerja sama secara wajar (*arm's length principle*), dalam hal pihak penyedia jasa TI merupakan pihak terkait dengan Bank.

b. Pernyataan kebijakan dari manajemen

Keputusan penggunaan penyedia jasa TI pada dasarnya harus mempertimbangkan faktor efisiensi dan risiko. Oleh karena itu, penggunaan penyedia jasa TI harus memenuhi prinsip-prinsip penggunaan penyedia jasa TI sebagaimana dimaksud dalam huruf a. Disamping itu, dalam:

1) penggunaan penyedia jasa TI harus mendapat persetujuan manajemen;
2) pemilihan penyedia jasa TI harus melalui proses uji tuntas*;*
3) pemilihan penyedia jasa TI untuk layanan TI harus melalui proses seleksi dari beberapa penyedia jasa; dan
4) perjanjian penyedia jasa TI harus memungkinkan adanya klausula kondisi pengakhiran perjanjian sesuai dengan masa perjanjian maupun sebelum masa perjanjian berakhir.

c. Peran dan tanggung jawab pihak-pihak yang terkait dengan penggunaan penyedia jasa TI

Sebagai bagian dari implementasi kebijakan, setiap peranan harus dialokasikan kepada manajemen Bank yang ditunjuk, dengan tanggung jawab:

1) memastikan penyedia jasa TI memenuhi kebutuhan dan sesuai dengan rencana strategis Bank;
2) memastikan Bank memiliki keahlian untuk mengawasi penyedia jasa TI;
3) mengevaluasi calon penyedia jasa TI berdasarkan ruang lingkup dan layanan yang akan diselenggarakan;

4) memastikan terdapat perjanjian pemeliharaan dengan penyedia jasa TI dalam hal kerja sama pengadaan TI;
5) memantau dan melakukan *risk assessment* secara berkala terhadap layanan yang diselenggarakan oleh penyedia jasa TI; dan
6) memastikan bahwa Otoritas Jasa Keuangan diberikan akses untuk melakukan pemeriksaan terhadap layanan yang diselenggarakan penyedia jasa TI.

9.2.2. Standar Penggunaan Penyedia Jasa TI

Bank harus memiliki standar mengenai penyelenggaraan TI kepada pihak lain yang paling sedikit mencakup:

a. standar pemilihan penyedia jasa TI sesuai dengan kompleksitas jasa TI yang dibutuhkan Bank;
b. standar pengelolaan penyedia jasa TI sesuai dengan ketentuan peraturan perundang-undangan dan tata kelola (*governance*) yang memadai; dan
c. standar isi perjanjian kerja sama dengan penyedia jasa TI, meliputi:
    1) cakupan pekerjaan atau jasa;
    2) biaya dan jangka waktu perjanjian kerja sama;
    3) hak dan kewajiban Bank maupun pihak penyedia jasa TI;
    4) jaminan pengamanan dan kerahasiaan data, terutama data nasabah. Data hanya bisa diakses oleh pemilik data (Bank);
    5) jaminan tingkat pelayanan (SLA), berisi mengenai standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service level*) dan target kinerja;
    6) SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penyedia jasa TI;
    7) laporan hasil pemantauan kinerja penyedia jasa TI yang terkait dengan SLA;
    8) batasan risiko yang ditanggung oleh Bank dan penyedia jasa TI, diantaranya:
        a) risiko perubahan ruang lingkup perjanjian;
        b) perubahan ruang lingkup bisnis dan organisasi perusahaan penyedia jasa TI;

c) perubahan aspek hukum dan regulasi; dan

d) aspek hukum yang meliputi hak cipta, paten dan logo atau merek (*trade mark*);

9) persetujuan Bank secara tertulis dalam hal pihak penyedia jasa TI melakukan pengalihan sebagian kegiatan (subkontrak) kepada subkontraktor. Selain itu, subkontraktor harus mempunyai standar penyelenggaraan TI yang memadai;

10) 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;

11) 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;

12) pengaturan mengenai pengamanan dalam pengiriman dokumen sumber (*source document*) yang diperlukan dari dan ke Pusat Data dan/atau Pusat Pemulihan Bencana. Pihak yang bertanggung jawab sebaiknya dilindungi asuransi yang cukup;

13) kesediaan diaudit baik oleh intern Bank, Otoritas Jasa Keuangan, dan/atau pihak ekstern yang ditunjuk oleh Bank maupun oleh Otoritas Jasa Keuangan dan tersedianya informasi untuk keperluan pemeriksaan, termasuk hak akses, baik secara *logic* maupun fisik terhadap data yang dikelola oleh penyedia jasa TI;

14) pihak penyedia jasa TI harus memberikan dokumen teknis kepada Bank terkait dengan jasa yang dikerjakan oleh penyedia jasa TI antara lain alur proses TI dan struktur Pangkalan Data (*Database*);

15) pihak penyedia jasa TI harus melaporkan setiap kejadian penting (*critical*) yang dapat mengakibatkan kerugian keuangan dan/atau mengganggu kelancaran operasional

Bank;

16) khusus untuk penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan Pemrosesan Transaksi Berbasis Teknologi Informasi, pihak penyedia jasa TI harus menyampaikan kepada Bank laporan keuangan terkini yang telah diaudit setiap tahun. Penyedia jasa TI menyampaikan hasil audit TI yang dilakukan auditor independen secara berkala terhadap penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi, kepada Otoritas Jasa Keuangan melalui Bank yang bersangkutan;
17) tanggung jawab penyedia jasa TI dalam menyediakan SDM yang memiliki kualifikasi dan kompetensi sesuai jasa yang disediakan agar operasional Bank tetap terjamin;
18) rencana pelatihan SDM, baik jumlah yang dilatih, bentuk pelatihan maupun biaya yang diperlukan. Pihak penyedia jasa TI harus melakukan transfer ilmu kepada Bank, sehingga terdapat personel satuan kerja TI di Bank yang memahami TI yang digunakan Bank terutama mengenai alur proses TI dan struktur Pangkalan Data (*Database*) dari sistem yang disediakan oleh pihak penyedia jasa TI tersebut;
19) kepemilikan dan lisensi;
20) jaminan dari penyedia jasa TI bahwa penyediaan jasa masih akan diberikan kepada Bank selama periode tertentu setelah implementasi;
21) perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal Otoritas Jasa Keuangan memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian;
22) sanksi dan penalti terhadap alasan-alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian;
23) kepatuhan pada hukum dan ketentuan peraturan perundang-undangan di Indonesia;
24) standar pengamanan sistem yang harus dipenuhi oleh

penyedia jasa TI;

25) standar tingkat pelayanan yang harus dipenuhi oleh penyedia jasa TI;
26) standar laporan pemantauan kinerja penyedia jasa TI; dan
27) standar perjanjian penyimpanan dokumen (*escrow agreement*).

9.2.3. Prosedur Penggunaan Penyedia Jasa TI

Bank harus memiliki prosedur penggunaan penyedia jasa TI yaitu prosedur pemilihan penyedia jasa TI yang paling sedikit mencakup:

a. Pendefinisian Kebutuhan

Pendefinisian kebutuhan paling sedikit memperhatikan:

1) Pendefinisian kebutuhan bisnis terhadap penggunaan jasa pihak penyedia jasa TI harus dilakukan sebelum Bank memutuskan menggunakan pihak penyedia jasa TI, diantaranya melalui:
   a) identifikasi secara spesifik mengenai fungsi atau aktivitas yang akan diserahkan penyelenggaraannya kepada pihak penyedia jasa TI;
   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.
2) Tahap pendefinisian kebutuhan di atas harus menghasilkan suatu dokumen yang berisi gambaran secara rinci mengenai keinginan Bank terhadap jasa yang akan dikerjakan oleh pihak penyedia jasa TI. Isi dari dokumen tersebut mencakup beberapa komponen berikut ini:
   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 penyedia jasa TI 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 pihak penyedia jasa TI;

f) jangka waktu, penghentian, dan isi minimal dari perjanjian; dan

g) perlindungan perjanjian terhadap kewajiban seperti pembatasan kewajiban dan ganti rugi serta asuransi.

Dalam hal penyelenggaraan kegiatan atau fungsi yang didefinisikan tersebut dipertimbangkan untuk dilakukan oleh pihak terkait Bank maka manajemen Bank harus memastikan bahwa persiapan yang dilakukan tidak berbeda apabila akan dilakukan oleh pihak tidak terkait dengan Bank.

b. Permintaan Proposal dari Penyedia Jasa TI

Proses pemilihan penyedia jasa TI dimulai dengan permintaan proposal dari penyedia jasa TI. 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 pihak penyedia jasa TI 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.

c. Uji Tuntas (*Due Diligence*) Penyedia Jasa TI

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 penyedia jasa TI mampu memenuhi kebutuhan Bank.

Pada saat uji tuntas (*due diligence*), Bank harus mempertimbangkan antara lain:

1) eksistensi dan sejarah perusahaan penyedia jasa TI;
2) kualifikasi, latar belakang, dan reputasi pemilik perusahaan penyedia jasa TI;
3) perusahaan lain yang menggunakan jasa yang sama dari penyedia jasa TI sebagai referensi;
4) kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual;
5) teknologi dan arsitektur sistem;
6) lingkungan pengendalian intern, sejarah pengamanan, dan cakupan audit;
7) kepatuhan terhadap hukum dan ketentuan peraturan perundang-undangan;
8) kepercayaan dan keberhasilan dalam berhubungan dengan sub kontraktor;
9) jaminan pemeliharaan;
10) kemampuan untuk menyediakan pemulihan bencana dan keberlanjutan bisnis;
11) penerapan manajemen risiko;
12) laporan hasil pemeriksaan 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.

d. Penentuan Penyedia Jasa TI

Dalam menentukan penyedia jasa TI, Bank harus memperhatikan antara lain:

1) Bank harus melakukan evaluasi atas penerapan manajemen risiko pihak penyedia jasa TI secara berkala untuk memastikan penggunaan pihak penyedia jasa TI tidak mengurangi tanggung jawab Bank dalam menerapkan manajemen risiko;
2) Bank harus memastikan bahwa laporan yang diperlukan untuk memantau kinerja pihak penyedia jasa TI telah memadai;
3) Bank harus melakukan analisis biaya dan manfaat untuk setiap alternatif yang akan dipilih;
4) Bank harus memastikan bahwa pihak penyedia jasa TI dapat menyampaikan hasil audit terkini atas TI yang dilakukan oleh pihak independen terutama untuk penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana;
5) Bank dapat memperoleh informasi dari berbagai sumber termasuk laporan tahunan pihak penyedia jasa TI dalam rangka memantau dan mengevaluasi kehandalan pihak penyedia jasa TI secara berkala, baik yang menyangkut kinerja, reputasi penyedia jasa TI, dan kelangsungan penyediaan layanan;
6) Bank harus memastikan akses terhadap Pangkalan Data (*Database*) dapat dilakukan oleh Otoritas Jasa Keuangan setiap saat baik untuk data terkini maupun untuk data yang telah lalu; dan
7) Bank harus menerapkan "hubungan kerja sama secara wajar *(arm's length principle*)" dengan pihak penyedia jasa TI termasuk pihak terkait dengan Bank. Bank harus melakukan proses seleksi dan didokumentasikan

e. Pembuatan Perjanjian Kerja Sama dengan Penyedia Jasa TI

Setelah memilih sebuah perusahaan penyedia jasa TI, manajemen membuat perjanjian tertulis dengan penyedia jasa TI sesuai standar perjanjian Bank. Dalam menyusun perjanjian, Bank harus memperhatikan hal-hal sebagai berikut:

1) isi penjanjian sesuai dengan standar perjanjian Bank;
2) melalui proses pembahasan dengan satuan kerja hukum; dan
3) mempertimbangkan adanya klausula khusus untuk pemutusan perjanjian sebelum berakhirnya perjanjian apabila penyedia jasa TI wanprestasi.

f. Klausula Khusus

Klausula khusus memperhatikan antara lain sebagai berikut:

1) Dalam perjanjian yang dibuat antara Bank dengan penyedia jasa TI harus dicantumkan klausula khusus mengenai kemungkinan mengubah, membuat perjanjian baru, atau mengambil alih kegiatan yang diselenggarakan oleh pihak penyedia jasa TI atau menghentikan perjanjian sebelum berakhirnya perjanjian. Termasuk dalam hal ini atas permintaan Otoritas Jasa Keuangan apabila diperlukan dengan pertimbangan bahwa penyelenggaraan oleh pihak penyedia jasa TI dapat mengganggu pelaksanaan tugas Otoritas Jasa Keuangan.
2) Bank mampu mengukur risiko dan efisiensi dari penyelenggaraan TI yang diserahkan kepada pihak penyedia jasa TI sehingga Bank dapat mengetahui secara dini bila terdapat kondisi-kondisi:
   a) memburuknya kinerja layanan TI oleh pihak penyedia jasa TI yang dapat berdampak signifikan pada kegiatan usaha Bank;
   b) tingkat solvabilitas pihak penyedia jasa TI tidak memadai, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan;
   c) terdapat pelanggaran terhadap ketentuan peraturan perundang-undangan mengenai rahasia Bank dan data pribadi nasabah; dan/atau
   d) terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan dalam rangka pengawasan yang efektif oleh Otoritas Jasa Keuangan.

3) Dalam hal Bank menemukan hal-hal sebagaimana dimaksud pada angka 2) maka Bank harus melakukan hal-hal:
   a) melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi tersebut di atas diketahui oleh Bank;
   b) memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan jasa TI apabila diperlukan; dan
   c) melaporkan kepada Otoritas Jasa Keuangan segera setelah Bank menghentikan penggunaan jasa TI sebelum berakhirnya jangka waktu perjanjian.
4) Untuk menjaga kelangsungan usaha Bank dalam hal penghentian penggunaan jasa TI dilakukan sebelum berakhirnya perjanjian maka Bank harus memiliki rencana tindak lanjut yang teruji dan memadai (*contingency plan*) dalam keadaan kahar (*force majeure*).

g. Penggunaan Penyedia Jasa TI di Luar Wilayah Indonesia

Bank yang merencanakan penggunaan penyedia jasa TI di luar wilayah Indonesia tidak boleh menghambat pengawasan atau pemeriksaan oleh Otoritas Jasa Keuangan. Sama halnya dengan penggunaan penyedia jasa TI domestik, penggunaan jasa TI pihak asing atau yang berlokasi di luar wilayah Indonesia harus melalui prosedur yang sama yaitu mulai dari uji tuntas, pemilihan penyedia jasa TI, pembuatan perjanjian dan pengawasan, namun karena terkait dengan perbedaan yurisdiksi maka terdapat persyaratan lain yang harus diperhatikan oleh Bank. Penggunaan pihak penyedia jasa TI di luar wilayah Indonesia harus terlebih dahulu mendapatkan persetujuan Otoritas Jasa Keuangan.

9.3. Proses Manajemen Risiko

9.3.1. Identifikasi Risiko

Identifikasi risiko paling sedikit memperhatikan hal-hal sebagai berikut.

a. Penggunaan pihak penyedia jasa TI lain dalam menyelenggarakan TI Bank dapat memberikan kontribusi

terhadap beberapa jenis risiko, yaitu:

1) risiko operasional yaitu ketidakmampuan penyedia jasa TI dalam memenuhi perjanjian;
2) risiko hukum yaitu ketidakpastian hukum atas perselisihan dengan pihak penyedia jasa TI, pihak ketiga, dan/atau tuntutan nasabah atas penyalahgunaan data nasabah oleh pihak penyedia jasa TI;
3) risiko reputasi yaitu ketidakpuasan nasabah karena ketidakmampuan penyedia jasa TI memenuhi SLA;
4) risiko stratejik yaitu ketidakcocokan TI yang digunakan Bank dengan tujuan dan rencana strategis Bank yang dibuat untuk mencapai tujuan tersebut;
5) risiko kepatuhan yaitu ketidakmampuan Bank memenuhi ketentuan peraturan perundang-undangan; dan
6) risiko negara (*country risk*) – kondisi di negara asing yang dapat mempengaruhi kemampuan penyedia jasa TI dalam memenuhi standar pemberian jasa.

b. Dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko, Bank harus mempertimbangkan:

1) terkait dengan aktivitas dan fungsi yang diselenggarakan oleh pihak penyedia jasa TI meliputi sensitivitas data yang diakses, dilindungi, atau dikendalikan oleh penyedia jasa TI, volume transaksi, dan tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis Bank;
2) terkait dengan penyedia jasa TI seperti misalnya kondisi keuangan, kompetensi tenaga kerja, perputaran manajemen dan tenaga kerja, pengalaman pihak penyedia jasa TI, dan profesionalitas; dan
3) terkait dengan 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.

9.3.2. Pengukuran Risiko

Setelah risiko diidentifikasi, Bank harus mengukur risiko tersebut untuk mengetahui tingkat risiko yang dihadapi. Pengukuran risiko

penggunaan penyedia jasa TI harus terintegrasi dengan pengukuran risiko terkait TI lainnya dengan menggunakan pendekatan pengukuran risiko yang sama.

Hasil pengukuran risiko penggunaan penyedia jasa TI ini harus menghasilkan suatu tingkat risiko yang selanjutnya menjadi salah satu parameter untuk penilaian risiko TI Bank secara keseluruhan.

9.3.3. 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.

a. Contoh tindakan mitigasi risiko yang dapat dilakukan Bank antara lain menerapkan kontrol untuk mengurangi kemungkinan terjadinya risiko, seperti:
   1) perjanjian penyedia jasa TI yang memadai;
   2) memantau kinerja penyedia jasa secara berkala; dan
   3) pemilihan penyedia jasa TI yang andal.
b. Tindakan mitigasi risiko lainnya adalah mengurangi dampak kerugian apabila risiko yang telah diidentifikasi terjadi seperti asuransi dan Rencana Pemulihan Bencana.
c. Bank harus memastikan bahwa risiko ketergantungan pada pihak penyedia jasa TI dapat dimitigasi sehingga Bank tetap mampu menjalankan bisnisnya apabila penyedia jasa TI mengalami wanprestasi, pemutusan hubungan, atau dalam proses likuidasi. Mitigasi risiko yang dapat dilakukan mencakup:
   1) memastikan bahwa pihak penyedia jasa TI memiliki Rencana Pemulihan Bencana sesuai dengan jenis, cakupan dan kompleksitas aktivitas atau jasa yang diberikan;
   2) secara aktif mendapatkan jaminan kesiapan Rencana Pemulihan Bencana milik pihak penyedia jasa TI seperti pengujian secara berkala atas Rencana Pemulihan Bencana;
   3) memiliki perjanjian penyimpanan program kode sumber (*escrow agreement)*, jika Bank tidak memiliki kode sumber

dari program aplikasi yang diselenggarakan oleh pihak penyedia jasa TI; dan

4) pemberian jaminan dari penyedia jasa TI kepada Bank bahwa kelangsungan aplikasi didukung oleh pejabat pengembang perangkat lunak dalam hal kode sumber tidak dimiliki oleh penyedia jasa TI.

d. Dalam rangka menjamin fungsi dan efektifivitas Rencana Pemulihan Bencana, Bank harus menyusun dan melakukan pengujian Rencana Pemulihan Bencana secara berkala, lengkap, dan mencakup hal-hal yang signifikan yang didasarkan atas jenis, cakupan, dan kompleksitas aktivitas atau kegiatan yang dilakukan oleh penyedia jasa TI. Disamping itu pihak penyedia jasa TI harus melakukan pengujian Rencana Pemulihan Bencana di pihak penyedia jasa sendiri untuk sistem atau fasilitas TI maupun pemrosesan transaksi yang diselenggarakan tanpa melibatkan pihak Bank. Hasil pengujian Rencana Pemulihan Bencana oleh pihak penyedia jasa TI tersebut digunakan Bank untuk mengkinikan Rencana Pemulihan Bencana yang dimiliki Bank.

9.3.4. Pengendalian Risiko Lainnya

Meskipun Bank maupun pihak penyedia jasa TI sudah menggunakan sistem yang canggih namun 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 hal-hal:

a. pihak penyedia jasa TI harus melakukan penelitian latar belakang para pegawainya;

b. memastikan kewajiban pihak penyedia jasa TI melakukan pengendalian keamanan terhadap seluruh fasilitas TI yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian;

c. memastikan pihak penyedia jasa TI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan Bank untuk masing-masing jenis data berdasarkan sensitivitas kerahasiaan data; dan

d. 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.

9.4. Pengendalian Intern dan Audit Intern

9.4.1. Pemantauan dan Pengawasan Penyedia Jasa TI

Dalam hal penyelenggaraan TI Bank dilakukan oleh pihak penyedia jasa TI, Bank tetap harus memiliki satuan kerja TI dan pejabat tertinggi yang memimpin satuan kerja TI.

Bank harus memiliki program pemantauan untuk memastikan penyedia jasa TI telah melaksanakan pekerjaan atau memberikan jasa sesuai dengan perjanjian. Sumber daya untuk mendukung program ini dapat bervariasi tergantung pada kritikalitas dan kompleksitas sistem, proses, dan jasa yang dikerjakan penyedia jasa TI.

Bank harus melakukan kaji ulang sebelum dan setelah pekerjaan penyedia jasa TI untuk memastikan bahwa kebijakan, standar, dan prosedur manajemen risiko Bank telah dilakukan secara efektif. Selanjutnya, *performance review* dan pencapaian SLA dilakukan secara berkala yang didokumentasikan dalam bentuk laporan. Pemantauan harus dilakukan terhadap laporan hasil pemeriksaan penyedia jasa TI.

9.4.2. Audit Intern

Bank melaksanakan fungsi audit terhadap pihak penyedia jasa TI secara berkala, baik dilakukan oleh audit intern Bank maupun pihak audit ekstern yang ditunjuk oleh Bank. Ruang lingkup audit sesuai dengan cakupan jasa sebagaimana yang tertuang dalam perjanjian. Area yang diaudit antara lain:

a. sistem TI;
b. keamanan data;
c. kerangka kerja pengendalian intern; dan
d. Rencana Pemulihan Bencana.

Bank harus memastikan bahwa Otoritas Jasa Keuangan atau pihak lain yang ditugaskan oleh Otoritas Jasa Keuangan memiliki hak akses ke penyedia jasa TI untuk mendapatkan catatan dan dokumen transaksi, serta informasi Bank yang disimpan atau

diproses oleh penyedia jasa TI serta hak akses terhadap laporan dan temuan audit terhadap penyedia jasa TI yang terkait dengan jasa TI.

BAB X PENYEDIAAN JASA TEKNOLOGI INFORMASI OLEH BANK

10.1. Pendahuluan

Dalam menyelenggarakan TI, Bank memerlukan infrastruktur TI yang memadai. Penyediaan infrastruktur tersebut dapat dilakukan sendiri oleh Bank, ataupun oleh penyedia jasa TI. 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 berperan sebagai penyedia jasa TI.

Bank dapat memberikan penyediaan jasa TI kepada Lembaga Jasa Keuangan (LJK) yang berada di bawah pengawasan Otoritas Jasa Keuangan dan/atau lembaga jasa keuangan lain di luar wilayah Indonesia. Jasa TI yang dapat diberikan Bank hanya terbatas pada penyediaan Pusat Data dan/atau Pusat Pemulihan Bencana termasuk jaringan komunikasi. Namun demikian, dalam rangka mendukung inklusi keuangan dan/atau meningkatkan efisiensi konglomerasi usaha, Bank dapat menyediakan jasa TI berupa penyediaan aplikasi kepada Bank lain dengan persetujuan Otoritas Jasa Keuangan.

10.2. Kebijakan, Standar, dan Prosedur Penyediaan Jasa TI

Dalam melakukan penyediaan jasa TI, Bank harus memenuhi ketentuan sebagaimana diatur dalam Pasal 25 POJK MRTI, serta memiliki kebijakan, standar, dan prosedur penyediaan jasa TI.

10.2.1. Kebijakan Penyediaan Jasa TI oleh Bank

Bank harus memiliki kebijakan mengenai penyediaan jasa TI oleh Bank, yang paling sedikit mengatur mengenai:

a. Prinsip-prinsip penyediaan jasa TI
    1) memenuhi persyaratan penyediaan jasa Teknologi Informasi tidak menjadi salah satu kegiatan pokok Bank;
    2) memenuhi prinsip kehati-hatian;
    3) memperhatikan analisa biaya dan manfaat (*cost and benefit analysis*);
    4) memenuhi ketentuan peraturan perundang-undangan; dan
    5) memenuhi prinsip hubungan kerja sama secara wajar

(*arm's length principle*).

Selain memenuhi prinsip penyediaan jasa TI di atas, Bank juga harus memastikan bahwa penyediaan jasa TI oleh Bank tidak mengganggu operasional Bank.

b. Pernyataan kebijakan dari manajemen

Keputusan penyediaan jasa TI pada dasarnya harus mempertimbangkan faktor efisiensi dan risiko. Oleh karena itu, penyediaan jasa TI harus memenuhi prinsip-prinsip penyediaan jasa TI sebagaimana tertulis pada huruf a dan harus:

1) mendapatkan persetujuan manajemen;
2) memiliki perjanjian penyediaan jasa TI yang memungkinkan adanya klausula 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.

10.2.2. Standar Penyediaan Jasa TI oleh Bank

Standar penyediaan jasa TI oleh Bank paling sedikit mencakup:

a. standar isi perjanjian kerja dengan penerima jasa TI;
b. jangka waktu perjanjian penyediaan jasa TI;
c. hak dan kewajiban Bank maupun penerima jasa TI;
d. jaminan pengamanan dan kerahasiaan data, terutama data nasabah. Data hanya bisa diakses oleh pemilik data.

   Khusus untuk menjaga kerahasiaan data Bank sebagai pengguna aplikasi maka Bank sebagai penyedia jasa TI harus memisahkan paling sedikit *table* dan/atau Pangkalan Data (*Database*) yang disesuaikan dengan arsitektur aplikasi Bank sebagai penyedia jasa TI;
e. jaminan tingkat pelayanan SLA, berisi mengenai standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service levels*) dan target kinerja;
f. SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penerima jasa TI;
g. batasan risiko yang ditanggung oleh Bank dan penerima jasa

TI, antara lain:

1) risiko perubahan ruang lingkup perjanjian;
2) perubahan aspek hukum dan regulasi; dan
3) aspek hukum yang meliputi hak cipta, paten, dan logo atau merek (*trade mark*);

h. 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;

i. kepemilikan dan hak cipta (*license*) dalam hal penyediaan jasa TI berupa aplikasi;

j. perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal Otoritas Jasa Keuangan memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian;

k. sanksi dan penalti terhadap alasan-alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian;

l. kepatuhan pada ketentuan peraturan perundang-undangan di Indonesia; dan

m. standar pengamanan sistem yang harus dipenuhi.

10.2.3. 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:

a. proses penilaian risiko yang timbul akibat penyediaan jasa TI oleh Bank; dan

b. penetapan dasar yang akan digunakan untuk mengidentifikasi pengukuran pengendalian risiko yang memadai.

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

1) cakupan dan karakteristik dari layanan dan teknologi yang digunakan;
2) jangka waktu, pengakhiran, dan isi minimal dari perjanjian;

dan

3) perlindungan perjanjian terhadap kewajiban seperti pembatasan kewajiban, ganti rugi, dan asuransi.

10.2.4. Pembuatan 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 memperhatikan hal-hal sebagai berikut:

a. melalui proses pembahasan dengan satuan kerja hukum; dan

b. mempertimbangkan adanya klausula khusus untuk pemutusan perjanjian sebelum berakhirnya perjanjian apabila penerima jasa TI wanprestasi.

Klausula khusus memperhatikan antara lain sebagai berikut:

1) Pencantuman klausula 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 akibat penyediaan 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 terhadap ketentuan peraturan perundang-undangan mengenai kerahasiaan data pribadi nasabah.

3) Dalam hal Bank menemukan hal-hal sebagaimana dimaksud pada angka 2) maka Bank harus melakukan hal-hal:

a) melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi tersebut di atas diketahui oleh Bank;

b) memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penyediaan jasa TI apabila diperlukan; dan

c) melaporkan kepada Otoritas Jasa Keuangan segera setelah Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian.

10.3. Proses Manajemen Risiko

10.3.1. Identifikasi Risiko

Identifikasi risiko paling sedikit memperhatikan hal-hal sebagai berikut.

a. Penyediaan jasa TI oleh Bank dapat memberikan kontribusi terhadap beberapa jenis risiko, sebagai berikut:
   1) risiko operasional yaitu ketidakmampuan Bank menyediakan jasa TI sesuai perjanjian;
   2) risiko hukum yaitu ketidakpastian hukum atas perselisihan dengan penerima jasa TI;
   3) risiko reputasi yaitu ketidakpuasan penerima jasa TI karena ketidakmampuan Bank memenuhi SLA; dan
   4) risiko kepatuhan yaitu ketidakmampuan Bank memenuhi ketentuan peraturan perundang-undangan.

b. Dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko, Bank harus mempertimbangkan:
   1) aktivitas dan fungsi penyediaan jasa TI meliputi sensitivitas data yang diakses, dilindungi, atau dikendalikan oleh Bank;
   2) penerima jasa TI seperti misalnya kondisi keuangan dan reputasi penerima jasa TI; dan
   3) 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.

10.3.2. Pengukuran dan Mitigasi Risiko

Setelah risiko diidentifikasi, Bank harus mengukur risiko tersebut untuk mengetahui tingkat risiko yang dihadapi. Pengukuran risiko penyediaan jasa TI harus terintegrasi dengan pengukuran risiko

terkait TI lainnya dengan menggunakan pendekatan pengukuran risiko yang sama.

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.

Contoh mitigasi risiko dalam penyediaan jasa TI:

1. Bank harus memiliki perjanjian penyediaan jasa TI yang memadai dan memantau penyediaan jasa TI secara berkala.
2. Bank mampu mengurangi dampak kerugian apabila risiko-risiko yang diidentifikasi telah terjadi.

Ditetapkan di Jakarta
pada tanggal 6 Juni 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

ttd

NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana

LAMPIRAN II
SURAT EDARAN OTORITAS JASA KEUANGAN
NOMOR 21 /SEOJK.03/2017

TENTANG
PENERAPAN MANAJEMEN RISIKO DALAM
PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

FORMAT LAPORAN PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DAFTAR ISI

Lampiran 2.1

LAPORAN KONDISI TERKINI PENGGUNAAN TEKNOLOGI INFORMASI

Nama Bank: .....
Alamat Kantor Pusat Bank: .....
Nomor Telepon.: .....

Nama Penanggung Jawab: .....
Kantor/Divisi/Bagian Penanggung Jawab:
.....
Alamat Penanggung Jawab: .....
Nomor Telepon.: .....

Tanggal Laporan : .....

DAFTAR LAPORAN KONDISI TERKINI
PENGGUNAAN TEKNOLOGI INFORMASI

2.1.1 Visi dan Misi Bank
2.1.2 Organisasi dan Manajemen
  2.1.2.1 Struktur Organisasi Bank dan Jumlah Sumber Daya Manusia Bank
  2.1.2.2 Struktur Organisasi Teknologi Informasi dan Jumlah Sumber Daya Manusia Teknologi Informasi
  2.1.2.3 Surat Keputusan Komite Pengarah Teknologi Informasi (*Information Technology Steering Committee*/ITSC) Terkini
  2.1.2.4 Risalah Rapat Komite Pengarah Teknologi Informasi (*Information Technology Steering Committee*/ITSC) 1 (satu) Tahun Terakhir
  2.1.2.5 Dokumen Rencana Strategis Teknologi Informasi (*Information Technology Strategic Plan*/ITSP)
2.1.3 Manajemen Risiko*)
  2.1.3.1 Penerapan Manajemen Risiko
  2.1.3.2 Struktur Organisasi Audit Intern Teknologi Informasi
  2.1.3.3 Audit Teknologi Informasi 1 (satu) Tahun Terakhir
2.1.4 Kebijakan, Standar, dan Prosedur Teknologi Informasi
2.1.5 Arsitektur Aplikasi
2.1.6 Daftar Aplikasi
2.1.7 Alur Proses Pelaporan
2.1.8 *Delivery Channel*
2.1.9 Jaringan Komunikasi
2.1.10 Pusat Data (*Data Center*) dan Pusat Pemulihan Bencana (*Disaster Recovery Center*)
2.1.11 Pengamanan Teknologi Informasi
2.1.12 Rencana Pemulihan Bencana (*Disaster Recovery Plan*)
2.1.13 Penyedia Jasa Teknologi Informasi
2.1.14 Biaya Teknologi Informasi

*) Manajemen Risiko adalah manajemen risiko operasional terkait teknologi informasi yang dapat mengganggu kelancaran operasional Bank.

Lampiran 2.1.1

VISI DAN MISI BANK

Visi Bank	
Misi Bank	
Arah kebijakan TI yang telah dilakukan selama 1 (satu) tahun untuk mendukung visi dan misi Bank:	
1. ... 2. ... 3. ... 4. ... 5. ...	

Lampiran 2.1.2

ORGANISASI DAN MANAJEMEN

Nomor Lampiran	Deskripsi	Keterangan
2.1.2.1	Struktur Organisasi Bank	*(dilampirkan)*
	Jumlah SDM Bank	*(diisi jumlah)*
2.1.2.2	Struktur Organisasi TI	*(dilampirkan)*
	Jumlah SDM TI	*(diisi jumlah)*
2.1.2.3	Surat Keputusan Komite Pengarah TI (ITSC) Terkini	*(dilampirkan)*
2.1.2.4	Risalah Rapat ITSC 1 (satu) Tahun Terakhir	*(dilampirkan)*
2.1.2.5	Dokumen Rencana Strategis TI (ITSP)	*(dilampirkan)*

Lampiran 2.1.3

MANAJEMEN RISIKO

Nomor Lampiran	Deskripsi	Keterangan
2.1.3.1	Penerapan Manajemen Risiko	*(dilampirkan)*
2.1.3.2	Struktur Organisasi Audit TI	*(dilampirkan)*
2.1.3.3	Audit TI 1 (satu) Tahun Terakhir	*(dilampirkan)*

Lampiran 2.1.3.1

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)*

*) Manajemen Risiko adalah manajemen risiko operasional terkait Teknologi Informasi yang dapat mengganggu kelancaran operasional Bank.

Lampiran 2.1.3.2

STRUKTUR ORGANISASI AUDIT INTERN TEKNOLOGI INFORMASI
(Diisi dengan gambar Struktur Organisasi Audit Intern TI; Sebutkan jumlah SDM Satuan Kerja Audit Intern-TI)

Lampiran 2.1.3.3

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*)

Lampiran 2.1.4

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) Dilengkapi dengan judul dokumen

(4) Diisi keterangan singkat mengenai dokumen

(5) Diisi dengan salah satu kategori:

- 301: Manajemen
- 302: Pengembangan dan Pengadaan
- 303: Operasional TI
- 304: Jaringan Komunikasi
- 305: Pengamanan Informasi
- 306: Rencana Pemulihan Bencana
- 307: Layanan Perbankan Elektronik
- 308: Penggunaan Pihak Penyedia Jasa TI
- 309: Penyediaan Jasa TI oleh Bank

(6) Diisi dengan salah satu jenis:

- K = Kebijakan
- S = Standar
- P = Prosedur

(7) Diisi tanggal revisi terakhir (DD-MM-YYYY)

Lampiran 2.1.5

ARSITEKTUR APLIKASI

Arsitektur Aplikasi
(Diisi dengan gambar Arsitektur Aplikasi)

Lampiran 2.1.6

DAFTAR APLIKASI

No.	Kategori Aplikasi	Nama Aplikasi	Deskripsi Fungsi Aplikasi	*Platform*	Pangkalan Data	Lokasi				*Backup Real Time*	*System Owner*	Pengembang Aplikasi (*Inhouse*/Pihak Penyedia Jasa)	Tanggal Implementasi (*Go Live*)	Kepemilikan (Sewa atau Beli Putus)
						Pusat Data	Penyelenggara Pusat Data	DRC	Penyelenggara DRC					
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
1	Contoh: 03	LOS	Memproses pengajuan kredit	"aaa"	"bbb"	Jakarta	Sendiri	Jakarta Medan	sendiri	Y	xxxxx	*inhouse*	xx-xx-xxxx	Sewa
2	Contoh: 01	PN2	*Core banking* di Kantor Cabang di WIT	"aaa"	"ccc"	Sentul	Sendiri	Sentul	sendiri	Y	xxxxx	*inhouse*	xx-xx-xxxx	Beli Putus

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 Perbankan Elektronik
- 07 : Tresuri
- 08 : Pembiayaan Perdagangan (*Trade finance*)

(3) Diisi dengan nama aplikasi

(4) Diisi dengan keterangan singkat mengenai fungsi aplikasi

(5) Diisi *platform* sistem operasi

(6) Diisi *database engine* yang digunakan

(7) Diisi dengan kota dan negara lokasi Pusat Data (*Data Center*/DC)

(8) Diisi dengan nama perusahaan penyelenggara DC atau "sendiri" (Bank)

(9) Diisi kota dan negara lokasi Pusat Pemulihan Bencana (*Disaster Recovery Center*/DRC) aplikasi

(10) Diisi perusahaan penyelenggara DRC atau "sendiri" (Bank)

(11) Diisi:
- "Y" Jika rekam cadang (*backup*) dilakukan secara *realtime*
- "T" Jika rekam cadang (*backup*) tidak dilakukan secara *realtime*

(15) Diisi "Sewa" atau "Beli Putus"

09 : Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU dan PPT)	(12)	Diisi unit bisnis yang mengelola aplikasi
10 : Manajemen sistem informasi pelaporan	(13)	Diisi: - "*Inhouse*", jika aplikasi dikembangkan sendiri oleh Bank - Nama Pihak Penyedia Jasa TI (PPJ TI), jika aplikasi dikembangkan oleh PPJ TI
11 : Manajemen risiko		
12 : Manajemen intern	(14)	Diisi dengan tanggal implementasi aplikasi (DD-MM-YYYY)

Lampiran 2.1.7

ALUR PROSES PELAPORAN

No.	Jenis Laporan	Aplikasi Sumber Data	Pengolahan Data	Aplikasi Pengolah Data yang Digunakan	Unit Pengolah Data	Unit Penanggung Jawab
(1)	(2)	(3)	(4)	(5)	(6)	(7)

Keterangan :

(1) Diisi dengan nomor urut

(2) Diisi nama laporan yang menjadi tujuan atau sasaran (contoh: Laporan Bulanan Bank Umum/LBU Form 01, Laporan Stabilitas Moneter dan Sistem Keuangan/LSMK, Sistem Layanan Informasi Keuangan/SLIK)

(3) Diisi nama aplikasi dari sumber data laporan (contoh: Modul CASA *core banking system*)

(4) Diisi: - "Manual", jika pengolahan data menjadi laporan dilakukan secara manual
- "Otomatis", jika pengolahan data menjadi laporan dilakukan menggunakan aplikasi

(5) Diisi nama aplikasi yang digunakan jika pengolahan data pada kolom (4) dilakukan secara otomatis

(6) Diisi unit bisnis yang melakukan pengolahan data

(7) Diisi unit yang bertanggung jawab terhadap laporan

Lampiran 2.1.8

DELIVERY CHANNEL

Delivery Channel	**Deskripsi**	**Jumlah**
Cabang	Jumlah Kantor Cabang	
	Jumlah Kantor Cabang Pembantu	
	Jumlah Kantor Kas	
	Jumlah Agen Layanan Keuangan Tanpa Kantor Dalam Rangka Keuangan Inklusif (Laku Pandai)	
ATM	Jumlah Mesin ATM Tunai:	
	- Tarikan Tunai	
	- Setoran Tunai	
	- Tarikan dan Setoran Tunai	
	Jumlah Mesin ATM Non Tunai	
EDC	Jumlah Mesin EDC	
	Frekuensi Transaksi	
	Nominal Transaksi Debit per Tahun	
Phone Banking	Jumlah Pengguna	
	Frekuensi Transaksi	
	Nominal Transaksi Debit per Tahun	
Internet Banking	Jumlah Pengguna	
	Frekuensi Transaksi	
	Nominal Transaksi Debit per Tahun	
Mobile Banking	Jumlah Pengguna	
	Frekuensi Transaksi	
	Nominal Transaksi Debit per Tahun	
Lainnya*) (Sebutkan)	Jumlah Pengguna	
	Frekuensi Transaksi	
	Nominal Transaksi Debit per Tahun	

*) Contoh:
1. SMS *Banking*
2. Uang elektronik
3. Dompet elektronik

Lampiran 2.1.9

JARINGAN KOMUNIKASI

TOPOLOGI JARINGAN KOMUNIKASI
(Diisi dengan gambar Topologi Jaringan Komunikasi)

Lampiran 2.1.10

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

DC/DRC 1

Keterangan	
Fungsi :	*(DC atau DRC)*
Penyelenggara :	
Alamat :	
Luas Area DC/DRC:	
Sertifikasi DC/DRC:	*(Hasil penilaian sesuai sertifikasi jika ada/ekuivalen berdasarkan assessment intern)*
Pengendalian fisik:	*(Penjelasan singkat mengenai pengendalian fisik di DC/DRC)*
Pengendalian lingkungan: - *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 :	*(DC atau DRC)*
Penyelenggara :	
Alamat :	
Luas Area DC/DRC:	
Sertifikasi DC/DRC:	*(Hasil penilaian sesuai sertifikasi jika ada/ekuivalen berdasarkan assessment intern)*
Pengendalian fisik:	*(Penjelasan singkat mengenai pengendalian fisik di DC/DRC)*

Pengendalian lingkungan: - *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)*

Lampiran 2.1.11

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)

Lampiran 2.1.12

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

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)*

Struktur Tim DRP
(Diisi dengan gambar Struktur Tim 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)*

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)*

Lampiran 2.1.13

PENYEDIA JASA TEKNOLOGI INFORMASI

13.1 Manajemen Penggunaan Pihak Penyedia Jasa TI

No.	Nama Pihak Penyedia Jasa	Alamat Pihak Penyedia Jasa TI	Pihak Terkait	Jasa yang Diberikan
(1)	(2)	(3)	(4)	(5)

Keterangan :

(1) Diisi dengan nomor urut
(2) Diisi dengan nama PPJ TI
(3) Diisi dengan alamat PPJ TI
(4) Diisi: - "Y", jika PPJ TI merupakan pihak terkait dengan Bank
- "T", jika PPJ TI bukan merupakan pihak terkait dengan Bank
(5) Diisi dengan daftar jasa yang diberikan PPJ TI kepada Bank, dapat berupa *support* aplikasi maupun infrastruktur (Contoh: *maintenance server core banking system* dan aplikasi pendukung "ABC")

13.2 Bank sebagai Pihak Penyedia Jasa TI

No.	Nama Pengguna Jasa	Alamat Pengguna Jasa TI	Pihak Terkait	Jasa yang Diberikan
(1)	(2)	(3)	(4)	(5)

Keterangan :

(1) Diisi dengan nomor urut
(2) Diisi dengan nama Pengguna Jasa TI
(3) Diisi dengan alamat Pengguna Jasa TI
(4) Diisi: - "Y" Jika Pengguna merupakan pihak terkait dengan Bank
- "T" Jika Pengguna bukan merupakan pihak terkait dengan Bank
(5) Diisi: - Penyelenggaraan Pusat Data (*Data Center*)
- Penyelenggaraan Pusat Pemulihan Bencana (*Disaster Recovery Center*)
- Penyediaan layanan aplikasi
- Lainnya (sepanjang diatur dalam POJK mengenai penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum)

Lampiran 2.1.14

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*/Capex)		
b. Biaya operasional (*operational expenditure*/Opex)		
2. Pembebanan ke neraca		

Keterangan:
(1.a) Diisi dengan penyusutan Capex ke laba/rugi
(1.b) Diisi dengan pembebanan Opex ke laba/rugi
(2) Diisi dengan tambahan Capex tahun berjalan ke neraca
*) Biaya dalam satuan mata uang Rupiah atau satuan mata uang lain disertai dengan nilai ekuivalen dalam mata uang Rupiah

Lampiran 2.2

LAPORAN RENCANA PENGEMBANGAN TEKNOLOGI INFORMASI

No.	Nama Aplikasi/ Infrastruktur Bank	Deskripsi	Kategori	Jenis Pengembangan	Pengembang	Pihak Penyedia Jasa TI Pihak Terkait	Lokasi		Waktu Rencana Implementasi	Estimasi Biaya		Keterangan*)
							DC	DRC		Capex	Opex	
(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 *Data Center*", "Penambahan kapasitas *bandwidth* jaringan"

(3) Penjelasan detil aplikasi/infrastruktur yang akan 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 Perbankan Elektronik
07 : Tresuri
08 : Pembiayaan Perdagangan (*Trade finance*)
09 : APU dan PPT
10 : Manajemen sistem informasi pelaporan
11 : Manajemen risiko
12 : Manajemen intern
49 : Aplikasi lainnya
51 : DC/DRC
52 : *Server* dan/atau *platform*
53 : Jaringan komunikasi data
54 : Sistem keamanan (*security system*)
99 : Infrastruktur lainnya

(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 intern Bank atau diisi "PPJ TI" jika dikembangkan oleh pihak ekstern Bank
(7) Diisi "ya" jika PPJ TI merupakan pihak terkait Bank, "tidak" jika PPJ TI bukan merupakan pihak terkait, "-" jika pengembangan dilakukan secara *inhouse* atau PPJ TI belum ditetapkan
(8) Diisi informasi nama kota dan negara lokasi DC dan DRC
(9) Diisi menggunakan periode triwulan yaitu TW1/TW2/TW3/TW4
(10) Diisi estimasi Capex dan/atau 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:
- dampak-dampak pengembangan TI, misalnya butuh penambahan SDM
- penjelasan keterkaitan pengembangan TI dengan rencana TI dalam Rencana Bisnis Bank

Catatan : Laporan Rencana Pengembangan TI ini tidak menghilangkan kewajiban Bank untuk menyampaikan laporan dan permohonan persetujuan sebagaimana diatur dalam Pasal 24 dan Pasal 32 POJK MRTI

Lampiran 2.3

PERMOHONAN PERSETUJUAN

Nama Bank: ..... Alamat Kantor Pusat Bank: ..... Nomor Telepon: .....
Nama Pelapor: ..... Kantor/Divisi/Bagian Pelapor: ..... Alamat Pelapor: ..... Nomor Telepon: .....
Tanggal Laporan: .....

Lampiran 2.3.1

PERMOHONAN PERSETUJUAN
RENCANA PENYEDIAAN JASA TEKNOLOGI INFORMASI OLEH BANK

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

	Ya	Tidak	

   b. Pusat Pemulihan Bencana.

	Ya	Tidak	

   c. Penyediaan layanan aplikasi.

	Ya	Tidak	

2. Pihak penerima jasa TI.
   a. Nama :
   b. Alamat :
   c. Deskripsi singkat usaha :
   d. Hubungan dengan Bank :
3. Informasi umum terkait layanan jasa TI yang akan disediakan 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: Laku Pandai	Aplikasi “ABC”	
2	Contoh: Layanan Perbankan Elektronik	*Mobile Banking*	
3	Contoh: Layanan Perbankan Elektronik	ATM	
…	…	…	
…	…	…	

4. Jika Bank menyediakan layanan 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. Lampirkan analisis biaya dan manfaat penyediaan layanan jasa TI yang dapat memperlihatkan manfaat bagi Bank melampaui biaya atas penyediaan layanan jasa TI.
6. Lampirkan analisis risiko terhadap penyediaan layanan jasa TI yang paling sedikit meliputi 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 layanan jasa TI.
7. Lampirkan konsep perjanjian antara Bank dengan pengguna jasa TI sebagaimana dipersyaratkan dalam POJK MRTI.

Lampiran 2.3.2

PERMOHONAN PERSETUJUAN
RENCANA PENERBITAN LAYANAN PERBANKAN ELEKTRONIK*)

1. Sistem, prosedur, dan kewenangan dalam penerbitan Layanan Perbankan Elektronik.
2. Uraian singkat atau penjelasan mengenai Layanan Perbankan Elektronik yang akan diterbitkan.
3. Kesiapan infrastruktur TI untuk mendukung produk masing-masing Layanan Perbankan Elektronik.
4. Lampirkan penjelasan mengenai sistem arsitektur TI dari Layanan Perbankan Elektronik yang akan diterbitkan dan bentuk koneksi dengan *core banking system.*
5. Hasil analisis dan identifikasi risiko yang melekat pada Layanan Perbankan Elektronik dan bentuk pengendalian pengamanan untuk mitigasi risiko tersebut antara lain untuk memastikan terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan tidak dapat diingkari (*non repudiation*).
6. Penjelasan aturan yang diterapkan Bank mengenai:
   a. dua faktor otentikasi *(two factor authentication)* yang akan digunakan;
   b. enkripsi yang akan digunakan; dan
   c. kata sandi (kriteria *numeric alphanumeric*, panjang kata sandi).
7. Uraian sistem informasi akuntansi yang akan diterapkan untuk Layanan Perbankan Elektronik yang akan diterbitkan.
8. Lampiran hasil analisis dan identifikasi risiko Layanan Perbankan Elektronik dalam bentuk identifikasi, pengukuran, pemantauan, dan mitigasi risiko dari Layanan Perbankan Elektronik yang baru diterbitkan, antara lain risiko operasional, hukum, dan reputasi.
9. Lampiran hasil pemeriksaan pihak independen yang memberikan pendapat atas karakteristik produk dan kecukupan pengamanan sistem TI terkait Layanan Perbankan Elektronik serta kepatuhan terhadap ketentuan peraturan perundang-undangan, standar yang ditetapkan, dan/atau praktik-praktik yang berlaku umum (*best practices*).

10. Uraian kesiapan struktur organisasi pendukung dan bentuk pengawasan yang melekat (*built in control*) yang akan diterapkan atas Layanan Perbankan Elektronik yang akan diterbitkan.
11. Hasil analisis bisnis mengenai proyeksi penerbitan produk baru dalam 1 (satu) tahun ke depan.

*) Permohonan persetujuan rencana penerbitan produk Layanan Perbankan Elektronik disampaikan kepada OJK paling lambat 2 (dua) bulan sebelum implementasi sebagaimana dipersyaratkan dalam POJK MRTI.

Lampiran 2.3.3

PERMOHONAN PERSETUJUAN
RENCANA PENYELENGGARAAN SISTEM ELEKTRONIK YANG DITEMPATKAN PADA PUSAT DATA (*DATA CENTER*) DAN/ATAU PUSAT PEMULIHAN BENCANA (*DISASTER RECOVERY CENTER*)
OLEH PIHAK PENYEDIA JASA DI LUAR WILAYAH INDONESIA *)

1. Rencana lokasi penyelenggaraan:
   a. Pusat Data.....
   b. Pusat Pemulihan Bencana .....
   c. Fungsi Sistem Elektronik.....

   Lampirkan data nama dan alamat serta kepemilikan penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana yang direncanakan.
2. Lampirkan ringkasan hasil pendefinisian kebutuhan dan uji tuntas (*due diligence*) yang telah dilakukan Bank dalam rencana penggunaan PPJ TI untuk menyelenggarakan Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia.
3. Berkaitan dengan ringkasan uji tuntas (*due diligence*) pada angka 2, sertakan hal-hal di bawah ini sebagai lampiran ringkasan:
   a. analisis Bank atas hasil audit TI yang dilakukan oleh pihak independen terhadap pengembangan sistem aplikasi yang ditawarkan dan sistem pengamanan pada fasilitas yang dimiliki oleh PPJ TI;
   b. analisis risiko Bank mengenai rencana menyerahkan penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana kepada PPJ TI antara lain risiko operasional, hukum, dan reputasi serta analisis *country risk*; dan
   c. analisis Bank mengenai kecukupan Pusat Pemulihan Bencana milik PPJ TI.
4. Lampirkan konsep perjanjian antara Bank dengan penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana di luar negeri yang memuat hal-hal sebagaimana dipersyaratkan dalam POJK MRTI.
5. Lampirkan ringkasan analisis risiko oleh PPJ TI atas penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana yang akan ditawarkan kepada Bank.
6. Lampirkan ringkasan analisis biaya dan manfaat penyelenggaraan TI oleh PPJ TI yang antara lain mencakup:
   a. manfaat bagi Bank melampaui biaya dibebankan oleh PPJ TI kepada Bank;

b. penilaian kecukupan dan kesesuaian sistem aplikasi yang akan digunakan dengan kebutuhan Bank;
c. analisis atas pengendalian pengamanan yang digunakan PPJ TI untuk memastikan terpenuhinya kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan keaslian (*authentication*); dan
d. analisis kinerja, reputasi, dan kelangsungan penyediaan layanan kepada para pengguna jasa TI.

7. Lampirkan gambar arsitektur TI saat ini dan yang direncanakan setelah penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana diserahkan kepada PPJ TI.
8. Lampirkan rencana pengawasan yang akan dilakukan Bank atas penyelenggaraaan Pusat Data dan/atau Pusat Pemulihan Bencana yang direncanakan.
9. Lampirkan 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.
10. Dalam hal Bank merupakan kantor cabang dari bank yang berkedudukan di luar negeri atau Bank yang dimiliki lembaga keuangan asing, lampirkan:
    a. Surat pernyataan dari otoritas pengawas lembaga keuangan di luar negeri bahwa PPJ TI merupakan cakupan pengawasannya;
    b. Surat pernyataan tidak keberatan dari otoritas pengawas setempat jika Otoritas Jasa Keuangan hendak melakukan pemeriksaan penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana tersebut;
    c. Surat pernyataan bahwa Bank secara berkala akan menyampaikan hasil penilaian yang dilakukan kantor Bank di luar negeri atau kantor induk Bank atas penerapan manajemen risiko pada PPJ TI. Surat pernyataan ini mencantumkan periodisasi yang direncanakan; dan
    d. Hasil penilaian oleh kantor Bank di luar negeri atau kantor induk Bank atas penerapan manajemen risiko yang dilakukan oleh PPJ TI.

11. Lampirkan rencana Bank mengenai:
    a. peningkatan kualitas pelayanan kepada nasabah; dan
    b. peningkatan kemampuan SDM yang berkaitan dengan penyelenggaraan TI yang digunakan oleh Bank.

*) permohonan persetujuan rencana penyelenggaraan Sistem Elektronik pada Pusat Data (*data center*) dan/atau Pusat Pemulihan Bencana (*disaster recovery center*) di luar wilayah Indonesia disampaikan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan sebelum penyelenggaraan kegiatan oleh PPJ TI efektif dioperasikan sebagaimana dipersyaratkan pada POJK MRTI.

Lampiran 2.3.4

PERMOHONAN PERSETUJUAN
RENCANA PENYELENGGARAAN PEMROSESAN TRANSAKSI BERBASIS TEKNOLOGI INFORMASI OLEH PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI DI LUAR WILAYAH INDONESIA*)

1. Uraian atau penjelasan dan *flow chart* dari standar prosedur pelaksanaan (*Standard Operating System)* dari produk dan aktivitas yang penyelenggaraannya akan diserahkan kepada PPJ TI.
2. Lokasi penyelenggaraan:
   a. Pusat Data.....
   b. Pusat Pemulihan Bencana .....
   c. Pemrosesan Transaksi Berbasis Teknologi Informasi.....

   Lampirkan data nama dan alamat serta kepemilikan penyelenggara Pemrosesan Transaksi Berbasis Teknologi Informasi yang direncanakan.
3. Lampirkan ringkasan hasil pendefinisian kebutuhan dan uji tuntas (*due diligence*) yang telah dilakukan Bank dalam rencana menggunakan PPJ TI untuk menyelenggarakan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar wilayah Indonesia.
4. Ringkasan uji tuntas (*due diligence*) pada angka 3, disertai dengan lampiran ringkasan mengenai:
   a. analisis Bank atas hasil audit TI yang dilakukan oleh pihak independen terhadap sumber daya TI (termasuk pengembangan sistem aplikasi yang ditawarkan, sistem operasi dan prosedur, dan sistem pengamanan pada fasilitas yang dimiliki) yang akan digunakan untuk memproses transaksi oleh PPJ TI;
   b. analisis risiko Bank atas rencana menyerahkan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi kepada PPJ TI antara lain risiko operasional, hukum, dan reputasi, serta analisis *country risk*; dan
   c. analisis Bank mengenai kecukupan Rencana Pemulihan Bencana (*Disaster Recovery Plan)* milik PPJ TI.
5. Lampirkan konsep perjanjian antara Bank dengan penyelenggara Pemrosesan Transaksi Berbasis Teknologi Informasi di luar wilayah Indonesia yang memuat hal-hal sebagaimana dipersyaratkan dalam POJK MRTI.

6. Lampirkan ringkasan analisis risiko oleh PPJ TI atas penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi yang akan ditawarkan kepada Bank.
7. Lampirkan ringkasan analisis biaya dan manfaat penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak lain yang antara lain mencakup:
   a. manfaat bagi Bank dibandingkan dengan biaya yang dibebankan oleh PPJ TI kepada Bank;
   b. penilaian kecukupan dan kesesuaian sistem aplikasi yang akan digunakan dengan kebutuhan Bank;
   c. analisis Bank atas pengendalian pengamanan yang digunakan pihak penyedia jasa untuk memastikan terpenuhinya kerahasiaan (*confidentiality)*, integritas (*integrity)*, ketersediaan (*availability),* dan keaslian (*authentication)*; dan
   d. analisis kinerja, reputasi, dan kelangsungan penyediaan layanan kepada para pengguna jasa TI.
8. Lampirkan gambar alur proses pelaporan dan informasi saat ini serta yang direncanakan setelah pemrosesan transaksi diserahkan kepada PPJ TI.
9. Bila Bank merupakan kantor cabang dari bank yang berkedudukan di luar negeri atau Bank yang dimiliki lembaga keuangan asing, perlu melampirkan:
   a. Surat pernyataan dari otoritas pengawas lembaga keuangan di luar negeri bahwa PPJ TI merupakan cakupan pengawasannya;
   b. Surat pernyataan tidak keberatan dari otoritas pengawas setempat apabila Otoritas Jasa Keuangan hendak memeriksa penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi tersebut;
   c. Surat Pernyataan bahwa Bank secara berkala akan menyampaikan hasil penilaian yang dilakukan kantor Bank di luar negeri atau kantor induk Bank atas penerapan manajemen risiko pada PPJ TI. Surat pernyataan ini mencantumkan periodisasi yang direncanakan.
   d. Hasil penilaian oleh kantor Bank di luar negeri atau kantor induk Bank atas penerapan manajemen risiko yang dilakukan oleh PPJ TI.

10. Lampirkan rencana pengawasan yang akan dilakukan Bank atas penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi yang direncanakan.
11. Lampirkan rencana Bank mengenai:
    a. peningkatan kemampuan SDM yang berkaitan dengan penyelenggaraan TI yang digunakan oleh Bank;
    b. peningkatan kemampuan SDM atas produk-produk yang ditawarkan Bank kepada nasabah;
    c. penerapan aspek perlindungan kepada nasabah atas produk yang pemrosesannya diserahkan kepada PPJ TI; dan
    d. peningkatan peran Bank bagi perkembangan perekonomian Indonesia melalui rencana bisnis.
12. Lampirkan 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.

*) permohonan persetujuan rencana penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh PPJ TI di luar wilayah Indonesia paling lambat 3 (tiga) bulan sebelum penyelenggaraan kegiatan oleh PPJ TI efektif dioperasikan sebagaimana dipersyaratkan pada POJK MRTI.

Lampiran 2.4

LAPORAN REALISASI TEKNOLOGI INFORMASI*)

Nama Bank: ..... Alamat Kantor Pusat Bank: ..... Nomor Telepon: .....
Nama Pelapor: ..... Kantor/Divisi/Bagian Pelapor: ..... Alamat Pelapor: ..... Nomor Telepon: .....
Tanggal Laporan: .....

Lampiran 2.4.1

REALISASI KEGIATAN SEBAGAI
PENYEDIA JASA TEKNOLOGI INFORMASI*)

1. Jenis layanan jasa TI yang disediakan oleh Bank.

a.

Penyelenggaraan Pusat Data	
Tanggal Realisasi	(dd/mm/yyyy)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerjasama	(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 kerjasama	(dd/mm/yyyy s.d dd/mm/yyyy)

c.

Jaringan Komunikasi	
Tanggal Realisasi	(dd/mm/yyyy)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerjasama	(dd/mm/yyyy s.d dd/mm/yyyy)

d.

Penyediaan Layanan Aplikasi	
Tanggal Realisasi	(dd/mm/yyyy)
Dokumen Perjanjian	(nomor dan tanggal dokumen)
Jangka waktu kerjasama	(dd/mm/yyyy s.d dd/mm/yyyy)

2. Pihak pengguna jasa TI.
   a. Nama :
   b. Alamat :
   c. Deskripsi singkat usaha :
   d. Hubungan dengan Bank :
3. Informasi umum terkait layanan jasa TI yang disediakan 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 Layanan Aplikasi
1	Contoh: Laku Pandai	Aplikasi "ABC"	
2	Contoh: Layanan Perbankan Elektronik	*Mobile Banking*	
3	Contoh: Layanan Perbankan Elektronik	ATM	
…	…	…	
…	…	…	

4. Lampiran perjanjian antara Bank dengan lembaga jasa keuangan pengguna yang sudah merealisasikan penggunaan layanan jasa TI.
5. Lampiran berita acara atas penyediaan layanan jasa TI yang disediakan oleh Bank sudah digunakan oleh lembaga jasa keuangan.
6. Lampiran hasil kajian pascaimplementasi (*Post Implementation Review*/PIR) atas penyediaan layanan jasa TI yang disediakan oleh Bank, antara lain mencakup:
   a. hasil kaji ulang kinerja sistem (*system performance review*);
   b. kesesuaian dengan *user requirement*;
   c. masalah yang terjadi dan solusi atau eskalasi atau langkah penyelesaian yang dilakukan; dan
   d. efektivitas pengamanan yang ditetapkan.

*) laporan realisasi kegiatan sebagai penyedia jasa TI disampaikan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah implementasi sebagaimana dipersyaratkan pada POJK MRTI.

Lampiran 2.4.2

REALISASI PENERBITAN
LAYANAN PERBANKAN ELEKTRONIK*)

1. Tanggal realisasi ... (diisi dengan format dd/mm/yyyy).
2. Uraian singkat atau penjelasan mengenai Layanan Perbankan Elektronik yang baru diterbitkan.
3. Lampiran penjelasan mengenai sistem arsitektur TI dari Layanan Perbankan Elektronik yang baru diterbitkan dan bentuk koneksi dengan *core banking system.*
4. Lampiran penjelasan mengenai bentuk pengendalian intern, khususnya pengendalian keamanan yang memastikan terpenuhinya aspek kerahasiaan (*confidentiality)*, integritas (*integrity)*, dan ketersediaan (*availability).*
5. Uraian kesiapan struktur organisasi pendukung dan bentuk pengawasan yang melekat (*built in control*) atas Layanan Perbankan Elektronik.
6. Lampiran kebijakan dan prosedur yang menjelaskan kesiapan infrastruktur TI Layanan Perbankan Elektronik.
7. Lampiran hasil kajian pascaimplementasi atas penggunaan TI terkait Layanan Perbankan Elektronik yang diterbitkan, yang tidak terbatas pada kaji ulang mengenai:
   a. kinerja sistem (s*ystem performance review*);
   b. komplain nasabah dan tindak lanjutnya;
   c. kesesuaian dengan *user requirement;*
   d. masalah yang terjadi beserta solusi atau eskalasi atau langkah penyelesaian yang dilakukan; dan
   e. efektivitas pengamanan yang ditetapkan.

*) laporan realisasi penerbitan produk Layanan Perbankan Elektronik disampaikan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah implementasi sebagaimana dipersyaratkan pada POJK MRTI.

Lampiran 2.4.3

REALISASI RENCANA PENYELENGGARAAN SISTEM ELEKTRONIK YANG DITEMPATKAN PADA PUSAT DATA DAN/ATAU PUSAT PEMULIHAN BENCANA DI LUAR WILAYAH INDONESIA*)

1. Tanggal realisasi ... (diisi dengan format dd/mm/yyyy).
2. Lokasi penyelenggaraan:
   a. Pusat Data.....
   b. Pusat Pemulihan Bencana .....
   c. Fungsi Sistem Elektronik.....
3. Lampiran fotokopi perjanjian antara Bank dan penyelenggara Pusat Data dan/atau Pusat Pemulihan Bencana.
4. Lampiran hasil analisis terkini atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya kerahasiaan (*confidentiality)*, integritas (*integrity)*, dan ketersediaan (*availability)* dalam penyelenggaraan yang diserahkan kepada pihak penyedia jasa TI.
5. Lampiran hasil pascaimplementasi atas penggunaan Pusat Data pihak penyedia jasa TI yang antara lain mencakup hasil kaji ulang mengenai:
   a. kinerja sistem (*system performance review*);
   b. kesesuaian dengan *user requirement*;
   c. masalah yang terjadi beserta solusi, eskalasi atau langkah penyelesaian yang dilakukan; dan
   d. efektivitas pengamanan yang ditetapkan.
6. Lampiran hasil pengujian atas penggunaan Pusat Pemulihan Bencana yang diselenggarakan PPJ TI tersebut.
7. Lampiran berita acara pengalihan Pusat Data dan/atau Pusat Pemulihan Bencana.
8. Lampiran gambar arsitektur TI terkini setelah penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana diserahkan kepada PPJ TI.
9. Uraian analisis risiko terkini Bank terhadap penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana oleh PPJ TI di luar wilayah Indonesia tersebut antara lain risiko operasional, hukum, dan reputasi, serta analisis *country risk*.

*) laporan realisasi penyelenggaraan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia disampaikan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah implementasi sebagaimana dipersyaratkan pada POJK MRTI.

Lampiran 2.4.4

REALISASI RENCANA PENYELENGGARAAN PEMROSESAN TRANSAKSI BERBASIS TEKNOLOGI INFORMASI KEPADA PIHAK PENYEDIA JASA DI LUAR WILAYAH INDONESIA*)

1. Uraian atau penjelasan dan *flow chart* dari standar prosedur pelaksanaan (*Standard Operating Procedure)* produk dan aktivitas Bank yang penyelenggaraannya diserahkan kepada pihak penyedia jasa TI.
2. Tanggal realisasi ... (diisi dengan format dd/mm/yyyy)
3. Lokasi penyelenggaraan:
   a. Pusat Data .....
   b. Pusat Pemulihan Bencana.....
   c. Pemrosesan Transaksi Berbasis Teknologi Informasi .....
3. Lampirkan fotokopi perjanjian antara Bank dan pihak penyedia jasa penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar wilayah Indonesia.
4. Lampirkan hasil pengujian atas penggunaan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar wilayah Indonesia.
5. Lampirkan berita acara pengalihan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar wilayah Indonesia.
6. Lampirkan hasil pascaimplementasi atas penggunaan PPJ TI dalam menyelenggarakan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar wilayah Indonesia yang antara lain mencakup hasil kaji ulang mengenai:
   a. kinerja sistem (*system performance review*);
   b. kesesuaian dengan *user requirement*;
   c. masalah yang terjadi beserta solusi atau eskalasi atau langkah penyelesaian yang dilakukan; dan
   d. efektivitas pengamanan yang ditetapkan.
7. Lampirkan gambar alur proses pelaporan dan informasi saat ini setelah penyelenggaraan diserahkan kepada PPJ TI.
8. Lampirkan hasil analisis atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya kerahasiaan (*confidentiality)*, integritas (*integrity)*, dan ketersediaan (*availability)* dalam penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi yang diserahkan kepada PPJ TI di luar wilayah Indonesia.

9. Lampirkan surat pernyataan dari PPJ TI sebagai pihak terafiliasi yang menyatakan kesediaan untuk diperiksa oleh Otoritas Jasa Keuangan terkait dengan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi.

*) Laporan realisasi Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak penyedia jasa TI di luar wilayah Indonesia disampaikan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah implementasi sebagaimana dipersyaratkan pada POJK MRTI.

Lampiran 2.5

LAPORAN INSIDENTIL MENGENAI KEJADIAN KRITIS, PENYALAHGUNAAN, DAN/ATAU KEJAHATAN DALAM PENYELENGGARAAAN TEKNOLOGI INFORMASI*)

Nama Bank: .....
Alamat Kantor Pusat Bank: .....
Nomor Telepon: .....
Nama Pelapor: .....
Kantor/Divisi/Bagian Pelapor: .....
Alamat Pelapor: .....
Nomor Telepon: .....
Tanggal Laporan: .....

1. Tanggal kejadian ... (dd/mm/yyyy).
2. Lampirkan kronologis dan evaluasi penyebab kejadian.
3. Terdapat unsur kesengajaan.

	Ya	Tidak	

4. Satuan kerja terkait termasuk orang yang dapat dihubungi lebih lanjut ...
5. Dampak atau akibat yang ditimbulkan.
   a. Kerugian keuangan
   b. Gangguan operasional
   c. Tidak terjaminnya kerahasiaan dan integritas data
6. Lampirkan rencana tindak lanjut Bank.

*) Kejadian kritis adalah kejadian yang menambah eksposur risiko secara signifikan. Penyalahgunaan atau kejahatan dalam penyelenggaraan TI adalah tindakan yang mengakibatkan timbulnya kerugian keuangan dan atau mengganggu kelancaran operasional Bank.

Lampiran 2.6

LAPORAN HASIL AUDIT TEKNOLOGI INFORMASI *)

Nama Bank:.....
Alamat Kantor Pusat Bank: .....
Nomor Telepon: .....
Nama Pelapor: .....
Kantor/Divisi/Bagian Pelapor: .....
Alamat Pelapor: .....
Nomor Telepon: .....
Tanggal Laporan: .....

1. Lampirkan detail anggota tim pelaksana audit TI.
2. Jika audit TI dilaksanakan oleh pihak ekstern, lampirkan perjanjian kerjasama 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.

*) 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, *contact person* di Bank yang menangani jasa penyelenggaraan TI tersebut dan informasi penting lainnya.

GLOSSARY

1. ***Acquirer*:** Bank atau lembaga selain Bank yang melakukan kegiatan alat pembayaran dengan menggunakan kartu yang dapat berupa *financial acquirer* dan/atau *technical acquirer*.

2. ***Access* - akses:** suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat keras atau perangkat lunak tertentu, seperti modem yang digunakan untuk membuka akses internet. Perangkat keras atau perangkat lunak tersebut selain untuk memberikan data juga digunakan untuk menerima data untuk disimpan.

3. ***Accountability* – akuntabilitas:** mekanisme untuk menilai tanggung jawab atas pengambilan keputusan dan tindakan.

4. ***Administrator Log*:** *file* pada komputer yang menyimpan informasi mengenai kegiatan administrator.

5. ***Automated Teller Machine* (ATM):** suatu terminal atau mesin komputer yang digunakan oleh Bank yang dihubungkan dengan komputer lainnya melalui komunikasi data yang memungkinkan nasabah Bank menyimpan dan mengambil uang di Bank atau melakukan transaksi perbankan lainnya.

6. ***Audit Trail* – Jejak Audit:** *file* pada komputer yang menyimpan informasi mengenai kegiatan pengguna (*user*) atau komputer, yang tersimpan secara kronologis, yang dapat digunakan untuk audit atau penelusuran.

7. ***Authentication* – Otentikasi:** kemampuan dari setiap pihak dalam transaksi untuk menguji kebenaran dari pihak lainnya.

8. ***Back Door*:** metode untuk melewati otentikasi normal atau *remote access* yang aman dari suatu komputer terhadap pengaksesan suatu sistem namun tidak teridentifikasi melalui pemeriksaan biasa.

9. ***Backup* – rekam cadang**: salinan dari dokumen asli atau cadangan dari mesin utama yang dapat digunakan apabila terjadi gangguan pada mesin utama. *Backup* dapat berupa *backup* data maupun *backup system*. *Backup* dapat ditempatkan secara *on site* di lokasi Pusat Data (*Data Center*) dan/atau *off site* di lokasi alternatif.

10. ***Backup Site*:** lokasi penyimpanan *backup* komputer dan *file* yang terpisah dengan Pusat Data.

11. ***Business Impact Analysis* (*BIA*):** proses untuk memastikan akibat yang ditimbulkan dari tidaktersedianya dukungan semua *resource* TI. Pada fase ini mencakup identifikasi beragam kejadian yang dapat mengakibatkan kelangsungan kegiatan operasional TI.

12. ***Contingency Plan*:** prosedur yang berisikan rencana atau langkah-langkah secara manual yang harus dilakukan oleh unit bisnis untuk menjalankan kegiatan operasional bisnis pada saat proses *recovery* sedang dilakukan.

13. ***Controller* (*Host-Front End*):** sejenis komputer mini yang berfungsi untuk mengontrol kinerja perangkat keras dan perangkat lunak yang ada pada suatu sistem seperti terminal komputer atau ATM, jaringan komunikasi atau sarana komputer lainnya.

14. ***Cost and Benefit Analysis* – Analisa Biaya dan Manfaat:** suatu analisis perbandingan antara biaya investasi dan keuntungan yang diperoleh Bank dari setiap alternatif pilihan penyedia jasa. Hasil analisis ini menjadi salah satu pertimbangan Bank untuk mengambil keputusan alih daya (*outsourcing*) atau pemilihan penyedia jasa TI.

15. ***Cybersquating*:** pendaftaran atau penggunaan alamat *website* atau nama domain dengan maksud buruk yaitu untuk menyalahgunakan atau memperoleh keuntungan dari penggunaan suatu merek dagang oleh pihak yang tidak berwenang.

16. ***Defacing*:** upaya *hacker* untuk menyerang dan mengubah tampilan atau isi suatu *website.*

17. ***Denial of Service Attack*:** serangan terhadap sistem TI sehingga menjadi lambat atau tidak dapat berfungsi sama sekali misalnya dengan membuat kapasitas (*bandwidth*) jaringan atau kapasitas (*disk space*) komputer seolah-olah telah terpakai penuh, gangguan pada *server* serta gangguan penyediaan jasa kepada sistem lain atau pengguna.

18. ***Digital Certificate*:** identitas elektronik yang digunakan untuk mengidentifikasi dan memverifikasi bahwa pesan tersebut dikirim oleh orang atau perusahaan yang berwenang dan hanya dibaca oleh pihak yang berwenang pula. *Digital certificate* diterbitkan oleh pihak ketiga yang disebut "*certification authority*".

19. ***Digital Signature*:** suatu informasi berupa tanda-tanda tertentu yang berbentuk digital yang dapat memastikan otentikasi pengirim, integritas data, dan tidak dapat diingkari.

20. ***Disposal Media Backup*:** proses penghancuran terhadap media *backup* yang sudah melewati masa retensi dan tidak digunakan.

21. ***Down Time*:** lamanya sistem tidak dapat berfungsi dan digunakan oleh pengguna karena adanya gangguan perangkat keras (*hardware*), perangkat lunak (*software*) dan komunikasi.

22. ***Due Diligence* – Uji Tuntas:** suatu proses untuk mendapatkan informasi paling lengkap mengenai penyedia jasa TI untuk menilai reputasi, kemampuan operasional, manajerial, kondisi keuangan, strategi pengembangan di masa mendatang dan kemampuan mengikuti perkembangan teknologi terkini.

23. ***Electronic Fund Transfer* (EFT):** transfer dana antar rekening melalui sistem pembayaran yang menggunakan media elektronik. EFT dapat dilakukan pada transaksi keuangan antara lain melalui telepon, dan terminal komputer.

24. ***Enkripsi*:** alat untuk mencapai keamanan data dengan menerjemahkannya menggunakan *password*. Enkripsi mencegah *password* atau *key* supaya tidak mudah dibaca pada file konfigurasi.

25. ***Escrow Agreement*:** suatu perjanjian yang memungkinkan pemberian hak kepada pembeli perangkat lunak untuk dapat memiliki kode sumber (*source code*) versi terkini dalam hal perusahaan pembuat sistem aplikasi tidak beroperasi lagi antara lain karena dipailitkan.

26. ***Exception Handling*:** mekanisme untuk menangani munculnya kondisi yang tidak diharapkan yang dapat mengubah alur normal suatu sistem aplikasi.

27. ***Firewall*:** peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data atau informasi melalui jaringan serta memisahkan jaringan privat dan publik. Peralatan ini dapat digunakan untuk melindungi komputer yang telah dikoneksikan dengan jaringan dari serangan yang dapat merusak komputer internal dan menyebabkan *data corruption* dan/atau *denial of service* bagi pengguna yang diotorisasikan.

28. ***Full System Backup*:** *system backup* yang mencakup keseluruhan sistem yang digunakan.

29. ***Gateway*:** titik dalam suatu jaringan yang berfungsi sebagai pintu masuk ke jaringan lain atau menghubungkan satu jaringan dengan jaringan lain. *Gateway* dapat berupa komputer yang mengatur dan mengendalikan lalu lintas jaringan.

30. ***Hardcopy*****:** salinan data atau informasi komputer dalam bentuk tercetak atau dikenal dengan *print out*.

31. ***Hardening* – pengaturan parameter:** merupakan proses atau metode untuk mengamankan sistem dari berbagai ancaman atau gangguan. Metode yang digunakan termasuk antara lain menonaktifkan layanan yang tidak diperlukan, serta *username* atau *login* yang tidak diperlukan, mengembangkan *intrusion detection system, intrusion prevention system* dan *firewall.*

32. ***Hub*****:** peralatan yang menghubungkan beberapa kabel pada jaringan dan meneruskan data atau informasi ke seluruh *address* yang berupa titik jaringan atau peralatan yang dituju.

33. ***Interoperability* – interoperabilitas:**

a. kemampuan perangkat lunak atau perangkat keras pada berbagai jenis mesin dari banyak vendor untuk saling berkomunikasi;
b. kemampuan untuk saling bertukar dan menggunakan informasi (biasanya dalam suatu jaringan besar yang terdiri beberapa jaringan lokal yang bervariasi).

34. ***IT Control*****:** pengendalian TI yang mencakup pengendalian umum dan pengendalian aplikasi yang terintegrasi untuk mendukung proses bisnis. Pengendalian umum TI diperlukan untuk memungkinkan diterapkannya fungsi pengendalian aplikasi.
Pengendalian umum Bank antara lain mencakup pengendalian di manajemen dan organisasi TI Bank, pengendalian akses baik fisik maupun *logic* dan pelaksanaan DRP. Pengendalian aplikasi diperlukan untuk memastikan kelengkapan dan akurasi dalam setiap tahap pemrosesan informasi. Pengendalian aplikasi diintegrasikan dengan sistem aplikasi yang digunakan untuk pemrosesan transaksi.

35. ***Key logger*****:** ancaman berupa perangkat lunak atau perangkat keras yang digunakan untuk memperoleh informasi (PIN, *password*) yang diketikkan pengguna pada *keyboard*.

36. ***Library*****:** kumpulan perangkat lunak atau data yang memiliki fungsi tertentu dan disimpan, serta siap untuk digunakan.

37. ***Logic Bomb*****:** suatu kode yang sengaja dimasukkan ke dalam suatu sistem perangkat lunak yang pada suatu kondisi tertentu akan melakukan serangkaian fungsi yang bersifat merusak.

38. ***Man-in-the-middle-attack*:** jenis serangan terhadap sistem teknologi informasi dimana penyerang (*hacker*) menyadap pesan yang dikirimkan pengirim kepada penerima dan/atau selanjutnya mengubah isi pesan dan mengirimkannya kembali kepada penerima. Penyerang (*hacker*) akan menggunakan program yang tampak seperti *server* bagi *client* dan tampak sebagai *client* bagi *server*.

39. ***Network interface* – antarmuka jaringan:** titik interkoneksi antara terminal pengguna, mesin, atau suatu jaringan dengan jaringan lain.

40. ***Non repudiation* – tidak dapat diingkari:** suatu cara untuk memastikan kebenaran pengirim dan penerima sehingga tidak ada pihak yang dapat menyangkal.

41. ***Offline* – luar jaringan:** sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

42. ***Off-the shelf*:** tersedia apa adanya, dibuat bukan berdasarkan pesanan khusus.

43. ***Outsourcing* – alih daya:** pengguna pihak lain (ekstern) dalam penyelenggaraan TI Bank yang menyebabkan Bank memiliki ketergantungan terhadap jasa yang diberikan pihak lain tersebut secara berkesinambungan dan/atau dalam periode tertentu.

44. ***Parallel Distributed*:** sistem terdistribusi yang terdiri dari sekumpulan komputer yang terhubung oleh jaringan, dengan *software* yang digunakan bersama sehingga seluruh komputer dapat berbagi sumber daya *hardware, software,* dan data. Sistem ini dapat menjembatani perbedaan geografis, meningkatkan kinerja, dan interaksi serta menekan biaya.

45. ***Password*:** kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer yang digunakan.

46. ***Patch*:** sekumpulan kode yang ditambahkan pada perangkat lunak untuk memperbaiki suatu kesalahan, biasanya merupakan koreksi yang bersifat sementara di antara dua keluaran versi perangkat lunak.

47. ***Patch Management*:** manajemen sistem yang meliputi proses memperoleh, pengujian dan instalasi berbagai *patch* yang digunakan untuk memperbaiki suatu program.

48. **Pengamanan Fisik:** suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap area komputerisasi serta peralatan atau fasilitas pendukung.

49. Pengamanan *Logic*: suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap sistem komputer dan informasi yang tersimpan di dalamnya yang antara lain meliputi penggunaan *user ID* dan *password*.

50. *Personal Identification Number* (PIN): rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi antara lain pengguna komputer, pengguna ATM, pengguna *internet banking,* dan pengguna *mobile banking*.

51. Perusahaan *Switching*: perusahaan yang memberikan pelayanan jasa perbankan elektronik kepada Bank dan lembaga jasa keuangan antara lain dalam pengelolaan perangkat keras komputer, jaringan telekomunikasi, informasi serta catatan transaksi nasabah Bank dan lembaga jasa keuangan tersebut.

52. *Phising*: salah satu bentuk teknik *social engineering* untuk memperoleh informasi rahasia seseorang secara ilegal.
Phising dapat dalam bentuk surat elektronik palsu yang seolah-olah berasal dari Bank atau perusahaan kartu kredit untuk memperoleh informasi seperti PIN dan *password*.

53. *Platform*: perangkat keras atau lunak seperti arsitektur komputer, sistem operasi atau bahasa pemrograman yang memungkinkan suatu aplikasi beroperasi.

54. *Point of Sales* (POS) atau *Electronic Data Capture* (EDC): suatu perangkat keras atau terminal komputer dapat berupa *cash register* atau terminal *debit/credit verification* yang membaca informasi pada pita magnetis kartu (*card's magnetic stripe)* kartu mengenai data transaksi di tempat penjualan (*merchant*), mentransmisikan data kepada *acquirer* untuk diverifikasi dan diproses.

55. *Power User*: *user id* yang memiliki kewenangan sangat luas.

56. *Public Key Infrastructure* (PKI): suatu pengolahan atau pengaturan dimana suatu pihak ketiga yang dapat dipercaya menyediakan pemeriksaan secara seksama dan memastikan keabsahan suatu identitas.

57. *Request for Proposal* (RFP): suatu proses permintaan proposal kepada para penyedia jasa sesuai dengan kebutuhan Bank untuk keperluan seleksi. Proposal yang disampaikan harus dapat menjawab secara rinci kebutuhan Bank yang sudah didefinisikan sebagaimana tertuang dalam dokumen *business requirement* atau *target operating model*.

58. ***Restore*:** mengembalikan pada fungsi atau kondisi semula sebelum terjadi *disaster*.

59. ***Restricted area*:** area yang hanya dapat dimasuki oleh orang yang telah mendapatkan hak akses.

60. ***Router*:** peralatan jaringan yang meneruskan suatu paket data atau informasi dengan memilih rute terbaik untuk ditempuh dalam menyampaikan data atau informasi tersebut.

61. ***Service Level Agreement* – Jaminan Tingkat Pelayanan:** bagian dari kontrak perjanjian dimana tingkat penyediaan layanan yang diharapkan para pihak ditetapkan biasanya mencakup pula standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service levels)* atau target waktu penyediaan layanan.

62. ***Softcopy*:** salinan data atau dokumen dalam bentuk *file* elektronik.

63. ***Source Code* – Kode Sumber:** instruksi program perangkat lunak yang ditulis dalam suatu format (bahasa) dan dapat dibaca oleh manusia.

64. ***Spoofing*:** suatu keadaan dimana seseorang atau suatu program dapat menyerupai orang lain atau program lain dengan cara memalsukan data dengan tujuan untuk mendapatkan keuntungan-keuntungan tertentu.

65. ***Spyware*:** perangkat lunak yang mengumpulkan informasi-informasi sensitif tentang pengguna tanpa sepengetahuan atau izin dari pengguna.

66. ***Stress Test*:** jenis *testing* dalam pengembangan yang menggunakan berbagai skenario misalnya dalam kondisi buruk.
    Stress test diperlukan menyangkut *performance, load balancing* khususnya untuk aplikasi yang kompleks.

67. ***Switch*:** peralatan dalam jaringan yang meneruskan paket informasi kepada alamat situs atau peralatan yang dituju.

68. ***System*:** suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran tertentu.

69. ***System Log*:** *file* pada komputer yang menyimpan informasi mengenai kegiatan sistem atau komputer.

70. ***Trojan Horse*:** program yang bersifat merusak yang disusupkan oleh *hacker* di dalam program yang sudah dikenal oleh pengguna replikasi atau distribusinya harus diaktivasi oleh program yang sudah dikenal oleh penggunanya melalui metode "*social engineering*".

71. ***Unit Test*****:** uji coba yang dilakukan oleh pengembang untuk menguji fungsionalitas dari modul-modul kecil dalam program perangkat lunak.

72. ***Upload*** **dan** ***Download*** **- unggah dan unduh:** transfer data elektronik antara dua komputer atau sistem yang sejenis.

73. ***User Acceptance Test*****:** uji coba akhir oleh pengguna untuk menguji keseluruhan fungsionalitas dan *interoperability* dari suatu sistem aplikasi.

74. ***User Log*****:** *file* di komputer yang menyimpan informasi mengenai kegiatan pengguna (*user*) seperti waktu *login* dan *log-out.*

75. Virus: program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi), dan tidak dapat mereplikasi sendiri penyebarannya, karena dilakukan oleh orang, seperti *copy*, biasanya melalui *attachement* surat elektronik, *game*, program bajakan, dan lain-lain.

76. ***Website*****:** situs web atau informasi yang disampaikan melalui suatu *web browser* atau sekumpulan *web page* yang dirancang, dipresentasikan dan saling terhubung untuk membentuk suatu sumber informasi dan/atau melaksanakan fungsi transaksi.

77. ***Worm*****:** program komputer yang dirancang untuk memperbanyak diri secara otomatis dan melekat pada surat elektronik atau sebagai bagian dari pesan jaringan.
Worm menyerang jaringan dan berakibat kepada penuhnya *bandwidth* yang terpakai sehingga menghambat laju pengiriman data pada jaringan.

Ditetapkan di Jakarta
pada tanggal 6 Juni 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

ttd

NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana