



BANK INDONESIA

Lampiran Surat Edaran Bank Indonesia Nomor: 9/30/DPNP Tanggal 12 Desember 2007

Lampiran 1

PEDOMAN PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

Direktorat Penelitian dan Pengaturan Perbankan

DAFTAR ISI

Kata Pengantar	ii
BAB I MANAJEMEN	1
BAB II PENGEMBANGAN DAN PENGADAAN	18
BAB III AKTIVITAS OPERASIONAL TEKNOLOGI INFORMASI	35
BAB IV JARINGAN KOMUNIKASI	45
BAB V PENGAMANAN INFORMASI	50
BAB VI BUSINESS CONTINUITY PLAN	61
BAB VII END USER COMPUTING	70
BAB VIII ELECTRONIC BANKING	75
BAB IX AUDIT INTERN TEKNOLOGI INFORMASI	91
BAB X PENGGUNAAN PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI	97
GLOSSARY	112
Lampiran 1.1. Contoh Penilaian Risiko	
Lampiran 1.2. Kategori Risiko pada <i>End User Computing</i>	

KATA PENGANTAR

Dalam rangka meningkatkan efisiensi kegiatan operasional dan mutu pelayanan Bank kepada nasabahnya, Bank dituntut untuk mengembangkan strategi bisnis Bank antara lain dengan memanfaatkan kemajuan Teknologi Informasi (TI). Pengembangan strategi tersebut selanjutnya mendorong investasi baru dalam TI yang digunakan dalam pemrosesan transaksi dan informasi. Kehandalan Bank mengelola TI menentukan keberhasilan Bank dalam menghasilkan suatu informasi yang lengkap, akurat, terkini, utuh, aman, konsisten, 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 misalnya risiko operasional, reputasi, legal, kepatuhan dan strategis. 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 menggunakan parameter yang lebih ketat sebagai tambahan dari hal-hal yang dikemukakan dalam pedoman. Sementara itu Bank dengan ukuran dan kompleksitas usaha yang relatif kecil dapat menggunakan parameter yang lebih ringan dari hal-hal yang dikemukakan dalam pedoman sepanjang Bank telah mempertimbangkan hasil penilaian terhadap risiko dalam aktivitas bisnis Bank, profil keamanan TI maupun hasil analisis atas *cost and benefit*. Bank juga diharapkan mengimplementasikan kerangka manajemen risiko ini dengan memperhatikan ketentuan perundangan yang berlaku, standar nasional dan internasional serta *best practices* untuk memastikan bahwa manajemen risiko yang memadai telah diterapkan.

BAB I MANAJEMEN

1.1. PENDAHULUAN

Operasional kegiatan usaha Bank termasuk pemrosesan transaksi dan pembukuan sangat tergantung pada keandalan Teknologi Informasi (TI). Informasi yang dihasilkan sangat dibutuhkan dalam pengambilan keputusan baik oleh pihak intern Bank maupun pihak ekstern. Untuk itu TI harus dikelola secara efektif guna memaksimalkan efektifitas penggunaannya dan agar risiko terkait dari teknologi yang diimplementasikan dapat dimitigasi.

Mengingat bahwa TI merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing Bank sementara dalam penyelenggaraannya mengandung berbagai risiko, maka Bank perlu menerapkan *IT Governance*. Penerapan *IT Governance* dilakukan melalui penyelarasan Rencana Strategis Teknologi Informasi dengan strategi bisnis Bank, optimalisasi pengelolaan sumber daya, pemanfaatan Teknologi Informasi (*IT value delivery*), pengukuran kinerja dan penerapan manajemen risiko yang efektif. Keberhasilan penerapan *IT Governance* sangat tergantung pada komitmen dewan komisaris dan direksi serta seluruh satuan kerja di Bank, baik penyelenggara maupun pengguna TI.

Sehubungan dengan hal itu diperlukan kebijakan yang memuat peran dan tanggung jawab dewan komisaris, direksi dan pejabat tertinggi TI dalam memastikan diterapkannya manajemen risiko TI secara efektif.

1.2. MANAJEMEN TEKNOLOGI INFORMASI

1.2.1. Peran dan Tanggungjawab Manajemen

1.2.1.1. Dewan Komisaris

Sesuai Undang-Undang Perseroan Terbatas, fungsi dewan komisaris adalah mengawasi kebijaksanaan direksi dalam operasional Bank serta memberi nasihat pada direksi. Dengan demikian dewan komisaris hendaknya memiliki komitmen, memahami dan berperan serta dalam kegiatan terkait TI. Tanggung jawab dewan komisaris mencakup antara lain:

- a. mengarahkan, memantau dan mengevaluasi Rencana Strategis TI dan kebijakan Bank terkait penyelenggaraan TI;
- b. melakukan pemantauan dan mengevaluasi kesesuaian antara kebijakan dengan penerapan manajemen risiko dalam penggunaan 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;
- d. melakukan evaluasi terhadap pengelolaan pengamanan yang andal dan efektif atas TI guna menjamin ketersediaan, kerahasiaan, keakuratan informasi.

1.2.1.2. Direksi

Wewenang dan tanggung jawab bagi direksi mencakup :

- a. menetapkan Rencana Strategis TI dan rencana pelaksanaan/pengembangan TI jangka pendek yang sejalan dengan rencana strategis dan rencana tahunan Bank;
- b. menetapkan kebijakan dan prosedur terkait penyelenggaraan TI yang memadai dan mengkomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna TI. Selanjutnya direktur yang membawahi Satuan Kerja Kepatuhan perlu meninjau ulang kebijakan dan prosedur tersebut untuk memastikan pemenuhan terhadap ketentuan perundangan yang berlaku;
- c. mereview, menyetujui dan memantau proyek-proyek teknologi yang berdampak secara signifikan terhadap operasional dan kondisi keuangan Bank;
- d. memastikan:
 - 1) TI yang digunakan Bank dapat mendukung perkembangan usaha, pencapaian tujuan bisnis Bank dan kelangsungan pelayanan kepada nasabah;
 - 2) tersedianya satuan kerja yang berfungsi mengelola TI yang diselenggarakan oleh Bank (atau digunakan oleh Bank bila diselenggarakan oleh pihak penyedia jasa TI);
 - 3) kebijakan dan prosedur serta standar yang ditetapkan telah diterapkan, dikaji ulang dan direvisi secara berkala;
 - 4) tersedianya Sistem Pengelolaan Pengamanan Informasi (*Information Security Management System*) yang efektif dan dikomunikasikan kepada seluruh pengguna dan penyelenggara Sistem Informasi;
 - 5) terdapat penerapan proses manajemen risiko dalam penggunaan TI yang dilaksanakan secara efektif dan memadai antara lain dengan:
 - a) menumbuhkan *risk awareness* dari manajemen;
 - b) memiliki dan mengkomunikasikan pemahaman yang jelas mengenai kriteria dan tingkat risiko yang dapat diterima oleh Bank (*risk appetite*) kepada satuan kerja pengguna dan penyelenggara TI;
 - c) memiliki pemahaman terhadap ketentuan yang berlaku;
 - d) mengkomunikasikan risiko signifikan secara transparan kepada satuan kerja pengguna dan penyelenggara TI yang menghadapi risiko tersebut; dan

- e) mengembangkan struktur organisasi beserta uraian tugas dan tanggung jawab yang dapat mengelola risiko yang dihadapi Bank secara komprehensif, sistematis dan terintegrasi.
- 6) tersedianya sumber daya manusia yang cukup dan kompeten sesuai dengan kebutuhan;
- 7) terdapat upaya peningkatan kompetensi sumber daya manusia terkait penyelenggaraan TI diantaranya melalui pendidikan/pelatihan yang memadai dan program edukasi untuk meningkatkan kesadaran atas pengamanan informasi;
- 8) terdapat sistem pengukuran kinerja proses penyelenggaraan TI yang paling kurang dapat:
 - a) mendukung proses pemantauan terhadap implementasi strategi;
 - b) mendukung penyelesaian proyek;
 - c) mengoptimalkan pendayagunaan investasi pada infrastruktur dan sumber daya manusia;
 - d) meningkatkan kinerja proses penyelenggaraan TI dan kualitas layanan penyampaian hasil proses kepada pengguna;
- 9) struktur organisasi manajemen proyek dari seluruh proyek terkait TI digunakan dengan maksimal;
- e. dalam hal Bank menggunakan jasa pihak lain, direksi harus memastikan bahwa Bank memiliki kontrak tertulis yang mengatur peran, hubungan, kewajiban, tanggung jawab dari semua pihak yang terikat kontrak tersebut, serta memiliki keyakinan bahwa kontrak tersebut merupakan perjanjian yang berkekuatan hukum dan melindungi kepentingan Bank.

1.2.1.3. Komite Pengarah Teknologi Informasi (*IT Steering Committee*)

Bank wajib memiliki Komite Pengarah TI yang bertujuan untuk membantu dewan komisaris dan direksi mengawasi kegiatan terkait TI. Komite sekurang-kurangnya terdiri dari:

- a. Direktur yang membawahi satuan kerja Teknologi Informasi;
- b. Direktur yang membawahi satuan kerja Manajemen Risiko;
- c. Pejabat tertinggi yang membawahi satuan kerja penyelenggara TI;
- d. Pejabat tertinggi yang membawahi satuan kerja pengguna utama TI;

Kewajiban untuk memiliki Komite Pengarah TI berlaku juga untuk Bank yang dimiliki oleh Bank Asing. Sedangkan untuk kantor cabang Bank Asing (KCBA), fungsi Komite Pengarah TI dapat dilaksanakan oleh fungsi sejenis yang berada di kantor pusat atau kantor regional.

Untuk dapat melaksanakan tugasnya, Komite Pengarah TI wajib memiliki *IT Steering Committee Charter* yang mencantumkan wewenang dan tanggung jawab komite.

Untuk dapat melakukan tugasnya secara efektif dan efisien, komite harus 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 adalah memberikan rekomendasi kepada direksi yang paling kurang mencakup:

- a. Rencana Strategis TI (*Information Technology Strategic Plan*) yang sesuai dengan rencana strategis kegiatan usaha Bank. Dalam memberikan rekomendasi, Komite hendaknya memperhatikan faktor efisiensi, efektifitas serta hal-hal sebagai berikut:
 - 1) rencana pelaksanaan (*road-map*) untuk mencapai kebutuhan TI yang mendukung strategi bisnis Bank. *Road map* terdiri dari kondisi saat ini (*current state*), kondisi yang ingin dicapai (*future state*) serta langkah-langkah yang akan dilakukan untuk mencapai *future state*;
 - 2) sumber daya yang dibutuhkan;
 - 3) keuntungan / manfaat yang akan diperoleh saat rencana diterapkan.
- b. perumusan kebijakan dan prosedur TI yang utama seperti kebijakan pengamanan TI dan manajemen risiko terkait penggunaan TI di Bank;
- c. kesesuaian proyek-proyek TI yang disetujui dengan Rencana Strategis TI. Komite juga menetapkan status prioritas proyek TI yang bersifat kritikal (berdampak signifikan terhadap kegiatan operasional Bank) misalnya pergantian *core Banking application*, *server production* dan topologi jaringan;
- d. kesesuaian pelaksanaan proyek-proyek TI dengan rencana proyek (*project charter*) yang disepakati dalam *service level agreement*. Komite hendaknya melengkapi rekomendasi dengan hasil analisis dari proyek-proyek TI yang utama sehingga memungkinkan direksi mengambil keputusan secara efisien;
- e. kesesuaian TI dengan kebutuhan sistem informasi manajemen yang mendukung pengelolaan kegiatan usaha Bank;
- f. efektivitas langkah-langkah minimalisasi risiko atas investasi Bank pada sektor TI dan bahwa investasi tersebut memberikan kontribusi terhadap tercapainya tujuan bisnis Bank;
- g. pemantauan atas kinerja TI, dan upaya peningkatannya misalnya dengan mendeteksi keusangan TI dan mengukur efektivitas dan efisiensi penerapan kebijakan pengamanan TI;
- h. upaya penyelesaian berbagai masalah terkait TI, yang tidak dapat diselesaikan oleh satuan kerja pengguna dan satuan kerja penyelenggara. Komite dapat memfasilitasi hubungan antara kedua satuan kerja tersebut;
- i. kecukupan dan alokasi sumber daya yang dimiliki Bank. Apabila sumber daya yang dimiliki tidak memadai dan Bank akan menggunakan jasa pihak lain dalam penyelenggaraan TI maka Komite Pengarah TI harus memastikan Bank telah memiliki kebijakan dan prosedur terkait.

1.2.1.4. Pejabat Tertinggi Yang Bertanggungjawab Membawahi Bidang TI

Dalam struktur organisasi, Bank harus menetapkan pejabat tertinggi yang hanya membawahi bidang TI. Jabatan tersebut dapat dibawah oleh direktur TI atau pimpinan satuan kerja TI sesuai dengan kompleksitas usaha di Bank. Wewenang dan tanggung jawab utama dari pejabat tertinggi TI tersebut minimal (namun tidak terbatas pada), mencakup hal-hal berikut:

- a. merumuskan kebijakan, rencana dan anggaran TI;
- b. menerapkan semua kebijakan TI dan rencana yang telah ditetapkan oleh direksi;
- c. memberikan dukungan pemberian jasa TI kepada satuan kerja pengguna untuk mencapai target bisnisnya secara responsif dan tepat waktu;
- d. memastikan setiap informasi yang dimiliki oleh satuan kerja pengguna TI mendapatkan perlindungan yang baik terhadap semua gangguan yang dapat menyebabkan kerugian akibat bocornya data/informasi penting;
- e. memastikan kecukupan dan efektifitas kebijakan dan prosedur TI serta penerapan manajemen risiko untuk mengidentifikasi, mengukur, menilai dan mengawasi risiko TI;
- f. memastikan terdapatnya pengawasan yang memadai dalam setiap pengembangan atau modifikasi sistem TI;
- g. memberikan kepada direksi laporan pelaksanaan TI secara periodik dan jika diperlukan dapat mengusulkan tindakan untuk mengatasi kelemahan TI yang telah ditemukan;
- h. menilai kinerja dari layanan TI di Bank, contohnya persentase berapa lama sistem mati (*downtime error*), pelanggaran keamanan, perkembangan proyek, penerapan perjanjian tingkat layanan (*Service Level Agreement - SLA*) antara satuan kerja TI dan satuan kerja pengguna atau pihak penyedia jasa TI;
- i. memastikan tindakan yang tepat telah dilakukan untuk memperbaiki temuan audit baik dari auditor intern maupun auditor ekstern atau berdasarkan laporan pemeriksaan Bank Indonesia;
- j. memastikan kecukupan sumber daya manusia baik dalam penyelenggaraan TI maupun dalam penerapan manajemen risiko ;
- k. apabila pejabat tertinggi yang secara langsung membawahi TI adalah seorang direktur maka yang bersangkutan berkewajiban mengawasi implementasi *budget* TI seperti pengadaan di bidang TI dan pelatihan. Apabila pejabat tertinggi bukan seorang direktur maka pengawasan kedua bidang tersebut dapat dilakukan oleh direktur yang membawahi;
- l. direktur TI bertanggung jawab terhadap penyusunan dan implementasi arsitektur TI dan rencana-rencana lain yang strategis yang mempengaruhi modal Bank secara signifikan, memastikan struktur organisasi manajemen proyek dari seluruh proyek terkait TI digunakan dengan maksimal;

- m. memastikan bahwa kontrak tertulis antara Bank dengan pihak penyedia jasa TI mencakup hal-hal yang telah diatur pada Bab X - Penggunaan Pihak Penyedia Jasa TI.

1.2.2. Rencana Strategis Teknologi Informasi

Rencana Strategis TI (*Information Technology Strategic Plan*) merupakan dokumen yang menggambarkan visi dan misi TI Bank, strategi yang mendukung visi dan misi tersebut dan prinsip-prinsip utama yang menjadi acuan dalam penggunaan TI untuk memenuhi kebutuhan bisnis dan mendukung rencana strategis jangka panjang Bank.

Sebelum menyusun Rencana Strategis TI Bank hendaknya melakukan analisis mengenai hal-hal yang terkait antara lain data terkait *Corporate Plan*, standar dan regulasi TI dan industri perbankan yang berlaku, trend teknologi, dan hasil *assessment* terhadap *current IT environment*.

Proses penyusunan dilakukan oleh satuan kerja penyelenggara TI, satuan-satuan kerja pengguna TI dan Komite Pengarah TI. Dokumen Rencana strategis TI mencakup antara lain hal-hal sebagai berikut:

- a. target perkembangan usaha Bank;
- b. standar-standar teknologi yang digunakan;
- c. ketentuan perundangan yang mendasari (antara lain mengenai rahasia bank, pengamanan, transparansi informasi produk dan penggunaan data pribadi nasabah);
- d. rencana kebutuhan akan aplikasi untuk produk dan aktivitas baru dan pengembangan produk dan aktivitas yang ada;
- e. biaya terkait dengan implementasi rencana;
- f. proses yang dibutuhkan dalam rangka efisiensi;
- g. pelayanan nasabah dan kualitas kinerja teknologi;
- h. analisis kemampuan sumber daya TI yang dimiliki Bank;
- i. infrastruktur TI yang optimal untuk masa depan;
- j. kemampuan untuk menyesuaikan dan mengintegrasikan dengan perkembangan teknologi baru; dan
- k. kemampuan untuk menyesuaikan dengan iklim perkembangan ekonomi Indonesia (secara makro).

Dalam penyusunan Rencana Strategis TI Bank hendaknya memperhatikan hal-hal sebagai berikut:

- a. kesesuaian arah dengan rencana strategis Bank secara keseluruhan;
- b. kesesuaian arah dengan strategi dan kegiatan masing-masing unit bisnis, kondisi pasar dan struktur demografi serta segmentasi nasabah;
- c. pemahaman manajemen mengenai peran dari TI dalam mendukung pelaksanaan kegiatan usaha Bank yang ada sekarang dan yang direncanakan;

- d. pemahaman manajemen mengenai hubungan antara sumber daya TI yang digunakan sekarang dan yang direncanakan dengan strategi dan rencana kerja dari satuan kerja pengguna TI;
- e. mempertimbangkan manfaat langsung dan tak langsung yang akan diperoleh dibandingkan biaya yang akan dikeluarkan untuk penggunaan teknologi;
- f. kebutuhan akan investasi baru dibidang teknologi.

1.2.3. Organisasi Teknologi Informasi

1.2.3.1. Fungsi Manajemen Risiko TI

Bank perlu memiliki fungsi penerapan manajemen risiko penggunaan TI dalam organisasi Bank yang melibatkan pihak-pihak yang memiliki risiko dan yang memantau (*oversee*) risiko serta yang melakukan test dan verifikasi.

Bank perlu memiliki kebijakan bahwa identifikasi, pengukuran dan pemantauan risiko setiap aktivitas/bisnis secara periodik dilakukan oleh Satuan Kerja Manajemen Risiko bekerja sama dengan satuan kerja penyelenggara TI dan satuan kerja pengguna TI. Selain itu untuk fungsi tertentu seperti fungsi pengamanan informasi dan fungsi *Business Continuity Plan* (BCP), pelaksanaan pengelolaan risiko tetap merupakan tanggung jawab dari tim kerja atau petugas yang melaksanakan fungsi-fungsi tersebut. Oleh karena itu manajemen Bank wajib memastikan pemantauan yang memadai dan pelaporan mengenai aktivitas terkait TI dan risikonya. Agar proses pemantauan dan pelaporan berfungsi optimal, maka audit internal maupun eksternal harus dapat melaksanakan fungsi test dan verifikasi dalam setiap pemeriksaan TI.

Untuk dapat menerapkan manajemen risiko pengamanan informasi secara optimal, Bank selain perlu memiliki fungsi yang melaksanakan prosedur pengamanan informasi sehari-hari juga perlu memiliki fungsi pengelola program pengamanan informasi dan pemantauan pengamanan secara *bank-wide*. Fungsi pertama hanya dapat melaksanakan prosedur yang telah ditetapkan dan tidak dapat mengambil keputusan untuk melakukan pengecualian atau mengubah prosedur dan standar pengamanan yang telah ditetapkan tersebut. Idealnya Bank perlu memisahkan kedua fungsi tersebut sehingga fungsi pengelola program pengamanan informasi (*Information Security Officer*) tersebut tidak bertanggungjawab terhadap satuan kerja TI melainkan kepada direksi. Dalam pelaksanaannya, Bank dapat menetapkan kebijakan dalam pelaksanaan kedua fungsi tersebut di atas yang disesuaikan dengan struktur organisasi dan kompleksitas usaha serta teknologi pendukung yang digunakan Bank.

1.2.3.2. Struktur Organisasi Satuan Kerja TI

Bank perlu memiliki struktur organisasi yang sesuai dengan kebutuhan penyelenggaraan dan penggunaan TI, dan sekurang-kurangnya memperhatikan hal-hal sebagai berikut:

- a. struktur organisasi secara spesifik menggambarkan garis kewenangan, pelaporan, tanggung jawab (dan jika dibutuhkan, orang pengganti) untuk setiap fungsi TI yang harus dimiliki;
- b. terdapat prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*) untuk mencegah seseorang mendapat tanggung jawab atas fungsi-fungsi yang berbeda dan kritis sedemikian rupa yang dapat menyebabkan kesalahan tidak mudah dideteksi. Misalnya adanya pemisahan pegawai yang bertanggung jawab melakukan administrasi pengamanan informasi (*security administrator*) dengan yang bertanggung jawab atas pengembangan dan yang melakukan kegiatan operasional TI;
- c. 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;
- d. untuk Bank berskala usaha yang relatif kecil atau kantor cabang di daerah terpencil, dimana tidak bisa menerapkan prinsip pemisahan tugas dan tanggung jawab yang memadai (*segregation of incompatible duties*) baik secara keseluruhan maupun sebagian, harus diganti dengan bentuk pengawasan lain atau *compensating controls* untuk pencegahan kesalahan penyelenggaraan TI. Dalam menentukan bentuk *compensating controls* yang akan diterapkan, Bank harus memperhatikan kepemilikan data, tanggung jawab otorisasi transaksi, dan hak akses ke data. Contoh *compensating controls*, antara lain *audit trail*, rekonsiliasi, *exception reporting*, *transaction log*, *supervisory review*, *independent review*. Sekalipun *compensating control* diterapkan, penyelenggaraan TI tetap harus berdasarkan prinsip kehati-hatian;
- e. penempatan personil mempertimbangkan kompetensi (pengetahuan dan keahlian) sumber daya manusia yang sesuai dengan posisi (jabatan/tugas);
- f. pembagian tanggung jawab dan penetapan target dirumuskan dengan baik di antara fungsi pengelolaan risiko dan bidang-bidang fungsional penyelenggaraan TI.

1.2.3.3. Manajemen Risiko TI pada Satuan Kerja Pengguna

Pimpinan dari satuan kerja pengguna TI juga mempunyai tanggung jawab atas penyelenggaraan dan penggunaan TI antara lain:

- a. memastikan adanya proses komunikasi berkelanjutan kepada satuan kerja TI mengenai kebutuhan terkait strategi bisnis Bank misalnya rencana penerbitan produk baru;
- b. menetapkan kebutuhan SIM dan mengkomunikasikannya ke satuan kerja TI;
- c. memastikan pegawai di satuan kerja pengguna berpartisipasi dalam proses pengujian yang dilakukan atas aplikasi yang akan digunakan oleh satuan kerja tersebut;
- d. memastikan para pengguna TI di satuan kerja pengguna mematuhi prosedur pengamanan yang telah ditetapkan untuk diterapkan.

Kepemilikan data/informasi berada pada satuan kerja pengguna. Sedangkan satuan kerja penyelenggara TI bertanggung jawab atas *custody of asset* yang berupa data/informasi. Untuk itu satuan kerja TI harus menetapkan standar dan prosedur *Custody of Corporate Assets* untuk mengelola data/informasi tersebut secara memadai.

1.2.4. Pengendalian Personil (*Personnel Control*)

Di samping membutuhkan pemilihan teknologi yang tepat, Bank juga membutuhkan personil yang memiliki kemampuan dan keahlian yang sesuai dan dapat mendukung pelaksanaan fungsi-fungsi TI secara maksimal. Karena itu Bank perlu melakukan pengendalian personil antara lain dengan menerapkan:

- a. penetapan prosedur untuk penerimaan pegawai baru, mutasi dan promosi, serta pemberhentian petugas TI. Prosedur ini berlaku untuk pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa. Untuk fungsi yang sensitif dalam pengelolaan TI diperlukan penelitian latar belakang calon pegawai dalam proses penerimaan;
- b. penetapan tugas, tanggung jawab, harapan/target secara transparan;
- c. penetapan standar penilaian kinerja, upah/gaji dan tunjangan, serta pensiun;
- d. program pendidikan dan pelatihan serta penilaian kinerja untuk mempertahankan dan meningkatkan kualitas para pegawai baik penyelenggara maupun pengguna TI.

Agar langkah-langkah pengendalian tersebut efektif, Bank perlu mempunyai rencana manajemen sumber daya manusia yang terintegrasi dengan Rencana Strategis TI.

1.2.5. Manajemen Proyek

Dalam hal Bank melakukan pengembangan dan pengadaan TI yang penting dan berskala besar, diperlukan suatu pengorganisasian dalam bentuk Manajemen Proyek. Hal ini diperlukan untuk memastikan bahwa sistem aplikasi yang diserahkan oleh satuan kerja TI untuk digunakan oleh satuan kerja pengguna, telah dikembangkan

dengan struktur yang baik dan telah mengakomodir 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/aplikasi TI di setiap proyek serta melaporkannya ke *Komite Pengarah TI*. Bentuk manajemen proyek dalam organisasi Bank disesuaikan dengan kompleksitas dan ukuran Bank yaitu dapat berupa suatu satuan kerja tetap atau bersifat *ad hoc*.

1.2.6. Sistem Informasi Manajemen (SIM)

Bank perlu memastikan terdapat suatu SIM yang dapat menghasilkan informasi yang diperlukan dalam rangka mendukung peran dan fungsi manajemen secara efektif. SIM harus dapat menyajikan informasi yang dibutuhkan secara lengkap, akurat, terkini, utuh, aman, benar, konsisten, tepat waktu, relevan dan dapat diaplikasikan untuk memudahkan proses perencanaan dan pengambilan keputusan yang mendukung usaha-usaha pencapaian strategis bisnis Bank.

Di samping 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/informasi ke berbagai satuan kerja sesuai jenis informasi, kualitas dan kuantitas maupun frekuensi dan waktu pengiriman laporan yang dibutuhkan;
- d. meningkatkan efektivitas dan efisiensi komunikasi di Bank;
- e. membantu Bank meningkatkan kepatuhan terhadap ketentuan perundangan;
- f. mendukung proses penilaian kinerja seluruh satuan kerja.

Kemajuan teknologi dapat meningkatkan ketersediaan informasi sehingga satuan kerja TI memegang peranan penting dalam efektivitas SIM Bank. Satuan Kerja TI menetapkan kebijakan, prosedur dan pengendalian manajemen *database* dan pembuatan laporan untuk membantu memastikan keefektifan SIM.

1.2.7. Dokumentasi

Manajemen Bank harus memastikan pengendalian internal maupun audit dapat melakukan test dan validasi atas kebijakan, proses, prosedur, standar dan *requirements* dalam pengelolaan TI. Untuk itu Bank harus memiliki dokumentasi kebijakan pengamanan dan manajemen risiko operasional yang jelas, lengkap dan dapat diaplikasikan khususnya yang terkait dengan risiko terkait TI di masing-masing satuan kerja pengguna TI.

1.3. MANAJEMEN RISIKO TERKAIT TEKNOLOGI INFORMASI

Kemampuan Bank memitigasi risiko TI tergantung dari hasil identifikasi, pengukuran, pengendalian dan pemantauan risiko-risiko terkait TI yang berpotensi mengancam keamanan dan operasional Bank.

Proses manajemen risiko terkait TI yang harus dilakukan setiap Bank mencakup empat hal penting yaitu:

- a. merencanakan penggunaan TI;
- b. menilai risiko terkait TI;
- c. menetapkan proses pengukuran dan pemantauan risiko terkait penyelenggaraan dan penggunaan TI;
- d. implementasi pengendalian TI.

1.3.1. Perencanaan Penggunaan TI

Sebagaimana dijelaskan di atas bahwa Bank wajib memiliki Rencana Strategis Teknologi Informasi (*Information Technology Strategic Plan*) yang mendukung rencana strategis kegiatan usaha Bank. Selanjutnya Rencana Strategis Teknologi Informasi yang akan diimplementasikan dalam satu tahun kedepan diungkapkan dalam Rencana Bisnis Bank yaitu dalam bagian Kebijakan dan Strategi Manajemen. Disamping itu apabila terdapat bagian dari Rencana Strategis TI tersebut yang terkait pengembangan produk dan aktivitas baru serta perubahan jaringan kantor bank maka harus diungkapkan pula pada bagian Pengembangan Produk dan Aktivitas Baru serta sub bab Perubahan Jaringan Kantor Bank. Setiap rencana pengeluaran terkait Rencana Strategis TI yang akan diimplementasikan pada tahun yang bersangkutan harus dimasukkan dalam proyeksi neraca di Rencana Bisnis.

Mengingat rencana strategis TI bersifat jangka panjang, maka untuk menjaga kesesuaian dengan perkembangan usaha Bank dan perkembangan TI maka Bank sebaiknya melakukan evaluasi secara berkala yang mencakup antara lain kinerja TI Bank serta tercapainya sasaran dan anggaran yang telah ditetapkan. Dengan demikian proyeksi neraca di Rencana Bisnis dapat lebih realistis dan berkesinambungan dari tahun ke tahun.

1.3.2. Penilaian Risiko yang Berkesinambungan

Kebijakan pengelolaan TI pada umumnya bertujuan untuk memastikan bahwa penyelenggaraan TI dapat mendukung pencapaian rencana bisnis Bank dan memastikan risiko yang terkait baik secara langsung maupun tidak langsung dengan penyelenggaraan TI tersebut dapat diatasi.

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

- a. *risk awareness* dari pejabat eksekutif dan direksi;
- b. pemahaman yang jelas mengenai *risk appetite* dari Bank;
- c. pemahaman terhadap ketentuan yang berlaku;
- d. transparansi dan integrasi tanggung jawab mengenai risiko-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 pengurus Bank atau menjalankan metode lain yang dapat meningkatkan kesadaran para pengguna TI akan risiko yang ada.

1.3.2.1. Jenis Risiko Terkait Teknologi Informasi

Bank wajib memiliki pendekatan manajemen risiko yang terpadu (terintegrasi) untuk dapat melakukan identifikasi, pengukuran, pemantauan dan pengendalian risiko secara efektif. Risiko terkait teknologi wajib dikaji ulang bersamaan dengan risiko-risiko lainnya yang dimiliki Bank untuk menentukan *risk profile* bank secara keseluruhan. Adapun risiko terkait penyelenggaraan TI yang utama adalah:

- a. Risiko Operasional

Risiko operasional melekat di setiap produk dan layanan yang disediakan Bank. Penggunaan TI dapat menimbulkan terjadinya risiko operasional yang disebabkan oleh antara lain ketidakcukupan/ketidaksesuaian desain, implementasi, pemeliharaan sistem atau komputer dan perlengkapannya, metode pengamanan, testing dan standar internal audit serta penggunaan jasa pihak lain dalam penyelenggaraan TI.

- b. Risiko Kepatuhan

Risiko kepatuhan dapat timbul bila Bank tidak memiliki sistem yang dapat memastikan kepatuhan Bank terhadap ketentuan yang berlaku bagi Bank seperti kerahasiaan data nasabah. Risiko kepatuhan dapat berdampak buruk terhadap reputasi serta citra Bank, juga berdampak pada kesempatan berusaha dan kemungkinan ekspansi.

- c. Risiko Hukum

Bank menghadapi risiko hukum yang disebabkan adanya tuntutan hukum, ketiadaan peraturan perundangan yang mendukung atau kelemahan perikatan seperti tidak dipenuhinya syarat sah suatu kontrak.

- d. Risiko Reputasi

Opini publik yang negatif dapat timbul antara lain karena kegagalan sistem yang mendukung produk, kasus yang ada pada produk Bank dan ketidakmampuan Bank memberikan dukungan layanan nasabah pada saat terjadi kegagalan sistem (*downtime*). Opini negatif ini dapat menurunkan kemampuan Bank memelihara loyalitas nasabah dan keberhasilan produk dan layanan Bank.

e. Risiko Strategis

Risiko ini timbul karena ketidakcocokan TI yang digunakan Bank dengan tujuan strategis Bank dan rencana strategis yang dibuat untuk mencapai tujuan tersebut. Hal ini karena kualitas implementasi maupun sumber daya yang digunakan TI kurang memadai. Sumber daya tersebut mencakup saluran komunikasi, *operating systems*, *delivery network*, serta kapasitas dan kapabilitas pengelola TI.

1.3.2.2. Penilaian Risiko

Dalam menggunakan teknologi, manajemen Bank harus menggunakan proses analisis yang ketat, menyeluruh, hati-hati & akurat, untuk mengidentifikasi dan mengkuantifikasi risiko serta memastikan pengendalian risiko diterapkan. Untuk itu penilaian risiko yang dilakukan Bank perlu dilakukan secara berkesinambungan dengan suatu siklus yang minimal mencakup empat langkah penting sebagai berikut:

- a. **Pengumpulan data/dokumen** atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko baik dari kegiatan yang akan maupun sedang 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 *review* rencana strategis bisnis, khususnya *review* terhadap penilaian risiko potensial;
 - 3) Hasil *due dilligence* dan pemantauan terhadap kinerja pihak penyedia jasa;
 - 4) Hasil *review* 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;
 - 6) Temuan-temuan audit terkait penyelenggaraan dan penggunaan TI.
- b. **Analisis risiko** berkaitan dengan dampak potensial dari tiap-tiap risiko, misalnya dari *fraud* di pemrograman, virus komputer, kegagalan sistem, bencana alam, kesalahan pemilihan teknologi yang digunakan, masalah pengembangan dan implementasi sistem, kesalahan prediksi perkembangan bisnis Bank.
- c. **Penetapan prioritas** pengendalian dan langkah mitigasi yang didasarkan pada hasil penilaian risiko Bank secara keseluruhan. Untuk itu Bank harus membuat peringkat risiko berdasarkan kemungkinan kejadian dan besarnya dampak yang dapat ditimbulkan serta mitigasi risiko yang dapat dilakukan untuk menurunkan eksposure 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, pengendalian kualitas termasuk *compensating control*.

1.3.3. Proses Pengukuran Dan Pemantauan Risiko

Seperti telah diuraikan sebelumnya terdapat beberapa jenis risiko yang terkait dengan penggunaan TI namun yang terbesar potensinya adalah risiko operasional. Hal ini perlu mendapat perhatian mengingat risiko operasional sulit dikuantifikasi. Bank perlu memperhatikan signifikansi dampak risiko yang telah diidentifikasi oleh Bank terhadap kondisi bank serta frekuensi terjadinya risiko. Metode yang dapat digunakan Bank dapat berupa kuantitatif maupun kualitatif tergantung kompleksitas usaha dan teknologi yang digunakan. Dalam metode kualitatif, besarnya dampak dan sering tidaknya kejadian (*likelihood*) dapat dijelaskan secara naratif atau dengan pemberian ranking. Contoh metode pengukuran yang sederhana antara lain dengan menggunakan *check list* atau menggunakan *subjective risk rating* seperti *High, Medium* atau *Low*. Bank harus menetapkan kriteria *High, Medium* atau *Low* dalam *risk rating* tersebut dan menerapkannya secara konsisten. Agar dapat memberikan hasil pengukuran risiko yang lebih sensitif, Bank dapat meningkatkan metode pemeringkatan risikonya dari 3x3 menjadi 4x4 sampai dengan 10x10. Contoh dari pemeringkatan menggunakan matriks risiko 5x5 adalah seperti dalam tabel berikut:

RATE OF OCCURENCE / LIKELIHOOD	IMPACT/ CONSEQUENCES / LOSS				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	Low	Medium	High	Very high	Very high
Likely	Low	Medium	High	Very high	Very high
Possible	Very low	Low	Medium	High	High
Unlikely	Very low	Very low	Low	Medium	Medium
Rare	Very low	Very low	Low	Low	Medium

Terdapat banyak program aplikasi pengukuran risiko yang menggunakan metode kuantitatif. Dalam metode ini digunakan data statistik mengenai kejadian dan besarnya dampak. Risiko diukur berdasarkan rata-rata tingkat kejadian (*rate of occurrence*) dan besarnya dampak dari kejadian (*the severity of the consequences/impact*). Beberapa bank menggunakan VAR untuk pengukuran risiko dengan metode kuantifikasi yang menganalisa *database likelihood* dan dampak dari kejadian-kejadian yang telah lalu.

Apabila Bank menggunakan paket sistem informasi manajemen risiko yang mencakup aplikasi pengukuran risiko sebagai alat bantu penerapan manajemen risiko dalam penggunaan TI, maka Bank harus memperhatikan asumsi yang digunakan dalam

sistem tersebut, serta pertimbangan bisnis (*business commonsense*) dan pertimbangan profesi (*professional dilligence*).

Agar risiko yang telah diidentifikasi dan dinilai atau diukur dapat dipantau oleh manajemen maka Bank perlu memiliki dokumentasi risiko (*Risk Documentation*) atau yang sering disebut sebagai *Risk Register*. Contoh pembuatan *Risk Register* tersebut dapat dilihat pada Lampiran 1.1. Contoh Penilaian Risiko. Bank dapat menetapkan komponen *Risk Register* yang berbeda dengan di Lampiran 1.1. namun paling kurang mencakup hal-hal sebagai berikut:

- 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);
- d. pengukuran atau pemeringkatan kemungkinan kejadian dan dampak setelah ACAT (*Residual Risk Assesment*).

Dalam dokumentasi *potential risk treatment* tersebut 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 risiko ini perlu dikinikn secara periodik.

Langkah-langkah penanganan risiko potensial yang dapat diambil Bank sesuai butir c di atas adalah sebagai berikut:

- a. Manajemen memutuskan untuk menerima risiko jika besarnya dampak dan tingkat kecenderungan masih dalam batas toleransi organisasi (*Accept*)

Contohnya adalah

- 1) dengan menetapkan Kriteria Penerimaan Risiko terkait dengan evaluasi dan penanganan risiko misalnya Nilai Risiko Akhir “*Low*”.

Kecenderungan	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Medium	Medium	High	High
	2	Low	Medium	Medium	Medium	High
	1	Low	Low	Medium	Medium	High
			1	2	3	4
Dampak						

- 2) 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.

- b. Organisasi memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan output yang sama untuk menghindari terjadinya risiko (*Avoid risk*).
Contohnya hak *privilege administrator* pada *user* yang menggunakan PC yang mengandung risiko akan adanya *malicious code* pada PC. Risiko ini dapat dihindari dengan tidak memberikan hak *privilege* pada *user* sehingga *user* tidak bisa merubah konfigurasi dan meng-*install software* pada PC.
- c. Organisasi memutuskan mengurangi dampak maupun kemungkinan terjadinya risiko (*Control / Mitigate*).
Contohnya penggunaan PC untuk mendukung proses bisnis organisasi mengandung risiko terjadinya *hacking* pada PC. Pengendalian risiko dilakukan dengan pemasangan fasilitas *firewall* untuk mencegah akses yang tidak terotorisasi.
- d. Organisasi memutuskan untuk mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga (*Transfer*).
Contohnya Penggunaan fasilitas ruangan atau gedung mengandung risiko terjadi kebakaran. Risiko ini ditangani dengan memindahkan risiko ke perusahaan asuransi yaitu dengan mengasuransikan fasilitas ruangan atau gedung.

1.3.4. Implementasi Pengendalian Teknologi Informasi

Manajemen harus menerapkan praktek-praktek pengendalian yang memadai sebagai bagian dari strategi mitigasi risiko TI secara keseluruhan.

Praktek-praktek pengendalian antara lain:

- a. penerapan kebijakan, prosedur, struktur organisasi termasuk alur kerjanya;
- b. 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;
- c. manajemen wajib menetapkan kebijakan dan prosedur serta standar (sistem pengelolaan pengamanan informasi) yang diperlukan Bank untuk melakukan pengamanan aset-aset terkait penyelenggaraan dan penggunaan TI termasuk didalamnya data atau informasi. Aturan lebih lanjut mengenai Pengamanan dapat dilihat pada Bab V - Pengamanan Informasi;
- d. manajemen harus mengevaluasi hasil kaji ulang (*review*) dan pengujian atas BCP untuk setiap bagian operasional yang kritis. Aturan lebih lanjut mengenai BCP dapat dilihat pada Bab VI - *Business Continuity Plan*. Seperti halnya dalam pengelolaan pengamanan informasi, BCP merupakan suatu strategi yang menyeluruh dan dilaksanakan oleh segenap satuan kerja yang ada di Bank;
- e. manajemen wajib memastikan terdapat kebijakan dan prosedur mengenai penggunaan pihak penyedia jasa. direksi harus memiliki pemahaman secara

menyeluruh atas risiko yang berhubungan dengan penggunaan jasa pihak penyedia jasa untuk sebagian atau semua operasional TI.

Untuk itu satuan kerja TI harus melakukan evaluasi kemampuan penyedia jasa untuk menjaga tingkat keamanan paling tidak 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 *outsourcing* operasional TI kepada pihak penyedia jasa TI. Aturan lebih lanjut dapat dilihat pada Bab X- *Outsourcing*;

- f. selain menerapkan bentuk pengendalian tersebut di atas, asuransi dapat digunakan sebagai pelengkap upaya memitigasi potensi kerugian dalam penyelenggaraan TI. Risiko yang perlu diasuransikan adalah *residual risk*. Bank hendaknya melakukan *review* secara periodik atas kebutuhan, cakupan dan nilai asuransi yang ditutup.

BAB II

PENGEMBANGAN DAN PENGADAAN SISTEM

2.1. PENDAHULUAN

Pengembangan dan pengadaan sistem mencakup pengelolaan sistem Teknologi Informasi yang tepat melalui proses identifikasi, pengembangan/pengadaan, implementasi dan pemeliharaan sistem Teknologi Informasi yang digunakan dalam proses bisnis Bank. Pengembangan dan pengadaan sistem dimaksud dapat berupa pengembangan perangkat lunak secara internal atau pembelian perangkat lunak, perangkat keras dan jasa pengembangan sistem dari pihak ketiga. Apabila pengelolaan dan pengendalian proses pengembangan dan pengadaan sistem lemah maka Bank dapat menghadapi berbagai risiko akibat adanya kesalahan (*error*), kejahatan (*fraud*) maupun produk atau layanan yang tidak tepat.

2.2. TUGAS DAN TANGGUNG JAWAB MANAJEMEN

Dalam melakukan pengembangan dan pengadaan Teknologi Informasi manajemen wajib melakukan langkah-langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan dan integritasnya serta mendukung pencapaian tujuan Bank, antara lain mencakup:

- a. menetapkan dan menerapkan prosedur dan metodologi pengembangan dan pengadaan Teknologi Informasi secara konsisten;
- b. menerapkan manajemen proyek dalam pengembangan sistem aplikasi yang utama;
- c. memastikan *testing* yang dilakukan pada saat pengembangan dan pengadaan suatu sistem telah memadai;
- d. memastikan sistem yang dikembangkan sesuai kebutuhan pengguna;
- e. memastikan kesesuaian satu sistem dengan sistem yang lain;
- f. melakukan dokumentasi sistem yang dikembangkan dan pemeliharaannya;
- g. memiliki manajemen perubahan sistem aplikasi;
- h. mengidentifikasi, mengukur dan mengendalikan secara memadai risiko-risiko yang dapat timbul terkait dengan pengembangan dan pengadaan sistem;
- i. memastikan bahwa Bank memiliki prosedur pengembangan sistem/aplikasi dalam keadaan darurat atau *emergency changes*.

2.2.1 Manajemen Proyek

Untuk pengembangan/pengadaan sistem aplikasi yang utama, Bank harus memiliki manajemen proyek untuk memastikan sistem aplikasi telah dikembangkan dengan struktur yang baik dan telah mengakomodir kebutuhan pengguna serta sesuai dengan

sistem Teknologi Informasi yang dimiliki Bank. Manajemen proyek dapat berbentuk tim kerja yang anggotanya paling kurang berasal dari satuan kerja TI dan satuan kerja pengguna. Sementara audit internal merupakan pihak independen yang memberikan masukan bagi kedua satuan kerja tersebut dalam memastikan kecukupan pengendalian di sistem aplikasi (*advisory capacity*).

2.2.2. Manajemen Perubahan Program

Yang dimaksud manajemen perubahan program adalah proses pengelolaan perubahan selama dalam pengembangan program, misalnya terjadi perubahan *user requirement*, perubahan teknologi pendukung yang digunakan.

Prosedur manajemen perubahan program harus dirumuskan, dijalankan dan didokumentasikan dengan baik. Permintaan perubahan harus diteliti sebelum disetujui untuk menentukan metode lain dalam melakukan perubahan, biaya perubahan, serta waktu yang dibutuhkan untuk aktivitas pemrograman. Penyebab sebenarnya yang menyebabkan perubahan harus diketahui dan didokumentasi dengan benar. Jejak audit (*audit trail*) dari semua perubahan yang diminta harus dipelihara. Aktivitas *programmer* harus diatur dan diawasi, dan semua pekerjaan yang ditugaskan harus diawasi dengan seksama terhadap tanggal pencapaian target.

2.3. KEBIJAKAN DAN PROSEDUR

Hal-hal yang perlu diperhatikan dalam kebijakan dan prosedur pengembangan dan pengadaan antara lain:

- a. Kebijakan dan prosedur pengembangan dan pengadaan sistem Teknologi Informasi sekurang-kurangnya meliputi hal-hal berikut:
 - 1) identifikasi dan analisis kebutuhan pengguna;
 - 2) pendefinisian kebutuhan (*user requirement*);
 - 3) rancangan system;
 - 4) pemrograman;
 - 5) pengujian;
 - 6) implementasi;
 - 7) *post implementation review*;
 - 8) pemeliharaan.
- b. Setiap pengembangan dan pengadaan sistem Teknologi Informasi harus selalu di bawah kendali satuan kerja Teknologi Informasi.
- c. Terhadap aplikasi yang dikembangkan oleh *vendor* atau dipengadaan dari pihak ketiga, Bank harus melakukan proses pemilihan *vendor*/pihak ketiga yang mengacu pada pedoman BI tentang *outsourcing* serta kebijakan dan prosedur intern. Bank juga harus memastikan kecukupan pelatihan dan manual yang disusun sebagai bagian dari kontrak antara Bank dan *vendor*.

- d. Kebijakan dan prosedur yang perlu dimiliki Bank dalam manajemen proyek antara lain:
- 1) Studi kelayakan harus dilakukan untuk mengetahui biaya dan manfaat dari pengembangan sistem, serta untuk menentukan apakah akan menggunakan sumber daya internal atau *outsourcing*;
 - 2) Persyaratan keamanan yang relevan harus dispesifikasikan secara jelas sebelum sistem baru dikembangkan atau diperoleh. Persyaratan keamanan tersebut harus sesuai dengan arsitektur keamanan informasi Bank secara keseluruhan;
 - 3) Perencanaan yang baik harus dilakukan untuk memastikan bahwa proyek akan memenuhi tujuannya;
 - 4) Bank harus melakukan pemisahan lingkungan (*environment*) untuk pengembangan, uji coba dan produksi, termasuk pembatasan akses ke masing-masing lingkungan;
 - 5) Jika sistem didukung atau dipelihara oleh *vendor*/pihak lain, analisis yang baik untuk pemilihan perangkat lunak harus dilakukan untuk memastikan kebutuhan pengguna dan bisnis dapat dipenuhi;
 - 6) Perjanjian kontrak antara Bank dan *vendor* harus diikat secara hukum;
 - 7) Bank harus menerapkan manajemen pemeliharaan untuk semua proses pengembangan dan pengadaan sistem yang telah diimplementasikan;
 - 8) Seluruh hasil (*deliverables*) pada setiap tahapan manajemen proyek harus didokumentasikan dengan baik.
 - 9) Bank harus memiliki rencana proyek yang formal meliputi hal-hal sebagai berikut:
 - a) identifikasi proyek, sponsor, dan manajer proyek;
 - b) tujuan proyek, informasi latar belakang dan strategi pengembangan;
 - c) deskripsi tanggung jawab utama dari tiap personil dalam manajemen proyek;
 - d) prosedur untuk mengumpulkan dan menyebarkan informasi;
 - e) kriteria hasil yang ditargetkan untuk masing-masing tahap pengembangan (*acceptance criteria*);
 - f) masalah keamanan dan pengendalian yang harus dipertimbangkan;
 - g) prosedur untuk memastikan manajer menilai, mengawasi, dan mengatur risiko internal dan eksternal dengan benar sepanjang siklus pengembangan;
 - h) *cut off date* untuk mengalihkan penggunaan sistem aplikasi dari yang lama ke versi terbaru hasil;
 - i) standar pengembangan yang akan digunakan untuk pengawasan proyek, pengendalian sistem dan kendali mutu (*quality assurance*);
 - j) jenis dan tingkatan dokumentasi yang harus dihasilkan oleh personil di setiap tahap 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 (testing plan) yang mengidentifikasi kebutuhan uji coba (testing requirement) dan jadwal prosedur uji coba;
 - n) rencana pelatihan yang mengidentifikasi kebutuhan pelatihan dan jadwal agar pegawai/karyawan dapat menggunakan dan memelihara aplikasi pasca implementasi.
- e. Kebijakan dan prosedur manajemen perubahan program yang harus dibuat Bank adalah prosedur modifikasi yang sekurang-kurangnya mencakup:
- 1) peninjauan ulang sebelum modifikasi dan otorisasi;
 - 2) pengujian sebelum modifikasi (dalam lingkungan pengujian yang terpisah);
 - 3) prosedur *backup* data dan *source code* 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 *source code* yang diubah;
 - e) Tanggal dan waktu modifikasi dilakukan; dan
 - 5) evaluasi setelah modifikasi.
- f. Dokumentasi yang harus dibuat selama proses modifikasi berlangsung terdiri dari:
- 1) informasi yang menjadi prioritas;
 - 2) identifikasi sistem, *database* dan satuan kerja yang terpengaruh;
 - 3) nama dari individu yang bertanggung jawab dalam membuat perubahan;
 - 4) kebutuhan sumber daya;
 - 5) prediksi biaya;
 - 6) prediksi tanggal penyelesaian;
 - 7) prediksi tanggal implementasi;
 - 8) pertimbangan potensi keamanan dan kehandalan;
 - 9) kebutuhan uji coba;
 - 10) prosedur implementasi;
 - 11) perkiraan *downtime* pada saat implementasi;
 - 12) prosedur *backup*;
 - 13) pengkinian dokumentasi (rancangan program dan *scripts*, topologi jaringan, manual pengguna, rencana kontinjensi, dll);
 - 14) dokumentasi penerimaan modifikasi dari semua satuan kerja terkait (pengguna, teknologi, *quality assurance*, keamanan, audit, dll); dan
 - 15) dokumentasi audit pasca implementasi (perbandingan antara harapan dan hasil).

2.4. MANAJEMEN RISIKO PENGEMBANGAN DAN PENGADAAN

Manajemen Bank bertanggung jawab terhadap manajemen risiko dari seluruh aktivitas yang terkait dengan pengembangan dan pengadaan sistem Teknologi Informasi.

2.4.1. Identifikasi Jenis Risiko Terkait Pengembangan dan Pengadaan

Proses pengembangan dan pengadaan sistem Teknologi Informasi yang dilakukan oleh Bank dapat memberikan kontribusi terhadap beberapa risiko, yaitu:

a. Risiko Operasional

Kesalahan, ketidakcukupan spesifikasi, kelemahan yang terdapat dalam sistem yang dikembangkan atau dibeli oleh Bank dapat menimbulkan risiko operasional antara lain terjadinya *fraud*, *error* dan ketidaksesuaian dengan kebutuhan. Risiko operasional tersebut juga dapat mempengaruhi risiko lainnya seperti risiko pasar, likuiditas, strategik dan reputasi.

b. Risiko Reputasi

Kesalahan, keterlambatan atau kelalaian dalam pengembangan sistem Teknologi Informasi yang digunakan Bank apabila mengganggu pelayanan kepada nasabah dapat secara signifikan mempengaruhi reputasi Bank.

c. Risiko Strategik

Kegagalan sistem yang dikembangkan dapat menghasilkan data dan informasi yang menyebabkan kesalahan pengambilan keputusan oleh manajemen.

d. Risiko Kepatuhan

Kegagalan dalam pengembangan atau akuisisi sistem Teknologi Informasi untuk mengikuti perubahan ketentuan dapat meningkatkan risiko kepatuhan bagi Bank.

Pada saat akan dilakukan pengembangan, Manajemen harus memperhatikan risiko terkait faktor berikut ini:

- a. ruang lingkup sistem yang akan dikembangkan meliputi sensitivitas data yang diakses, dilindungi atau dikendalikan, *volume* transaksi, dan tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis Bank;
- b. terkait dengan teknologi yang digunakan meliputi kehandalan (*reliability*), keamanan (*security*), ketersediaan (*availability*), dan ketepatan waktu (*timeliness*) serta kemampuan mengikuti perkembangan teknologi dan perubahan ketentuan.

2.4.2. Pengendalian Risiko Pada Pengembangan Sistem Aplikasi

Dalam melakukan pengembangan Bank harus menentukan metodologi yang akan digunakan. Salah satu bentuk metodologi yang dapat digunakan oleh Bank adalah *System Development Life Cycle* (SDLC). Dalam SDLC, tahap pengembangan suatu

sistem aplikasi bagi menjadi inisiasi, perencanaan, pendefinisian kebutuhan, desain, pemrograman, uji coba, implementasi, kaji ulang pasca implementasi, dan pemeliharaan. Contoh metodologi pengembangan lain yang dapat digunakan oleh bank antara lain seperti *agile software development*, *Rapid Application Development (RAD)*, dan metode lain yang telah menjadi standarisasi pengembangan sistem. Namun demikian, setidaknya dalam pelaksanaan dengan metode pengembangan lainnya, Bank mengacu pada tahapan yang ada pada pedoman ini.

2.4.2.1. Tahap Inisiasi dan Perencanaan

Tahap inisiasi diawali dengan identifikasi kebutuhan untuk menambahkan, menyempurnakan atau memperbaiki suatu sistem yang diminta oleh pengguna melalui suatu proposal. Tahap inisiasi ini terdiri dari langkah-langkah antara lain sebagai berikut:

- a. penyusunan proposal yang berisi identifikasi kebutuhan pengguna untuk menambahkan, menyempurnakan atau memperbaiki suatu sistem, tujuan dan manfaat yang diharapkan serta bagaimana sistem yang akan dikembangkan dapat mendukung strategi bisnis;
- b. evaluasi proposal oleh manajemen;
- c. persetujuan prinsip pengembangan/pengadaan sistem baru atau perubahan sistem;
- d. studi kelayakan proyek yang antara lain pertimbangan bisnis, kebutuhan fungsional, faktor-faktor yang mempengaruhi proyek dan analisis manfaat dan biaya (*cost and benefit analysis*);
- e. persetujuan manajemen atas dokumen studi kelayakan;
- 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.

2.4.2.2. Tahap Pendefinisian Kebutuhan Pengguna (*User Requirement Definition*)

Berdasarkan dokumen studi kelayakan yang telah disetujui secara tertulis oleh manajemen, manajer proyek dapat membentuk tim guna menyusun *requirement definition* secara detail sebagai dasar dimulainya pengembangan sistem aplikasi. Pada tahapan ini, seluruh kebutuhan pengguna dikumpulkan berdasarkan contoh-contoh dokumen/form, spesifikasi proses dan sistem yang ada saat ini, *interview* dengan pengguna akhir dan riset serta analisis terhadap ketentuan/regulasi yang berlaku. Tahap pendefinisian kebutuhan pengguna ini terdiri atas:

- a. Pengumpulan kebutuhan (*Requirements Elicitation*), merupakan proses pengumpulan informasi mengenai tujuan pengembangan sistem, *output/* hasil yang diinginkan, bagaimana sistem dapat mengakomodir kebutuhan bisnis proses dan bagaimana sistem akan digunakan.
- b. Analisis Kebutuhan (*Requirements Analysis*) 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. Hasil analisa kebutuhan digunakan untuk menghasilkan alur bisnis proses (seperti *Business Process Flows*, *Use Cases Modeling* dan *Data Flow Diagrams*) yang dapat memperjelas pemahaman mengenai kebutuhan dan solusinya, baik bagi pengguna maupun pengembang.
- c. Spesifikasi Kebutuhan (*Requirements Specification*) merupakan proses yang mendeskripsikan fungsional sistem yang akan dikembangkan, baik dari segi perangkat lunak maupun perangkat keras pendukung serta desain *database*. Spesifikasi kebutuhan harus lengkap, komprehensif, dapat diuji, konsisten, jelas dan merinci kebutuhan input, proses dan output yang dibutuhkan.
- d. Pengelolaan Kebutuhan (*Requirements Management*) merupakan proses yang dilakukan oleh tim proyek untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat pengembangan berjalan.

2.4.2.3. Tahap Merancang (*Desain*) Sistem

Tahap ini mengkonversikan kebutuhan informasi, fungsi dan jaringan yang teridentifikasi selama tahap inisiasi dan perencanaan menjadi spesifikasi desain yang akan digunakan pengembang. Salah satu teknis desain adalah dengan menggunakan prototipe yang mengembangkan desain maket dari bagian aplikasi seperti tampilan layar, struktur data dan arsitektur sistem. Pengguna akhir, perancang, pengembang, *database* administrator dan *network* administrator harus melakukan kaji ulang dan memilih desain yang diprototipekan dalam suatu proses *iteratif* (berulang-ulang) sampai disepakati desain yang akan digunakan. Personil auditor, *security* dan *quality assurance* harus dilibatkan dalam proses *review* dan persetujuan di atas.

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. Pada tahap ini, audit intern berpartisipasi memberikan masukan pengendalian yang harus diterapkan dalam sistem aplikasi. Tahap ini diperlukan untuk meningkatkan keamanan, integritas dan kehandalan sistem dengan memastikan informasi input, proses dan output yang terotorisasi, akurat, lengkap dan aman.

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

- a. Pengendalian Input
Minimal dapat mencakup pengecekan terhadap validitas/kebenaran data, *range data/ parameter*, dan duplikasi data yang diinput;
- b. Pengendalian Proses
Memastikan proses bekerja secara akurat dan dapat menyimpan informasi atau menolaknya. Pengendalian proses yang dapat dilakukan secara otomatis oleh sistem mencakup paling kurang *Error Reporting, Transaction Log*, pengecekan urutan, *backup file*;
- c. Pengendalian Output
Memastikan sistem mengelola informasi dengan aman dan mendistribusikan informasi hasil proses dengan tepat serta menghapus informasi yang telah melewati masa retensi.

2.4.2.4. Tahap Pemrograman

Dalam tahap ini dilakukan konversi spesifikasi desain menjadi program yang dapat dijalankan. Selama tahap ini, Bank harus membuat rencana uji coba yang harus dilakukan. Selain itu, Bank juga harus mengkinikan rencana migrasi, implementasi dan pelatihan pengguna akhir, operator dan dokumentasi manual pemeliharaan.

- a. Standar Pemrograman
Dalam standar pemrograman dijelaskan antara lain mengenai tanggung jawab *programmer* aplikasi dan *programmer* sistem. Manajer proyek harus memahami secara keseluruhan mengenai proses pemrograman untuk memastikan tanggung jawab *programmer* telah sesuai, antara lain:
 - 1) Membatasi akses programmer terhadap data, program, utilitas, dan sistem di luar tanggung jawabnya. Pengendalian *librarian* dapat digunakan untuk mengelola akses tersebut.
 - 2) Pengendalian versi merupakan metode yang secara sistematis menyimpan kronologis dari salinan program yang disempurnakan serta menjadi salah satu dokumentasi program.
- b. Dokumentasi
 - 1) Bank harus mengelola dan memelihara dokumentasi yang detail untuk setiap sistem aplikasi baik yang dikembangkan sendiri maupun produk/perangkat lunak yang dibeli atau dikembangkan pihak lain yaitu mencakup:
 - a) deskripsi detail aplikasi;
 - b) dokumentasi pemrograman;

- c) format-format yang digunakan (format database, format tampilan dan informasi);
 - d) standar penamaan;
 - e) pedoman bagi operator dan pedoman untuk pengguna akhir.
- 2) Dokumentasi harus dapat mengidentifikasi standarisasi pengembangan, seperti narasi sistem, alur sistem, pengkodean khusus sistem, pengendalian intern dalam dokumen aplikasi itu sendiri.
 - 3) Dalam hal produk/perangkat lunak dibeli atau dikembangkan oleh pihak lain, manajemen harus memastikan *review* telah dilakukan baik secara intern maupun oleh pihak independen bahwa dokumentasi produk/ perangkat lunak telah sesuai dengan standar minimum dokumentasi Bank.

2.4.2.5. Tahap Uji Coba

Bank harus melaksanakan beberapa rangkaian uji coba untuk memastikan keakuratan dan berfungsinya sistem aplikasi sesuai kebutuhan pengguna serta hubungan sistem aplikasi tersebut dengan sistem aplikasi lain (*interoperability*) yang telah digunakan oleh Bank. Segala 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 serta pelatihan. Ujicoba yang dapat dilakukan oleh Bank antara lain adalah:

- a. *Unit Testing*,
- b. *System Integration Testing*,
- c. *Stress Testing*,
- d. *User Acceptance Test*.

User Acceptance Test (UAT) merupakan uji coba akhir yang dilakukan oleh pengguna akhir terhadap sistem/ aplikasi yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem apakah telah sesuai dengan kebutuhan pengguna pada *user requirement definition* sebelum memutuskan implementasi dapat dilakukan. Pada tahap ini audit intern dapat ikut melakukan pengujian dengan tetap menjaga tingkat independensi apabila audit intern perlu meyakini ketersediaan, kecukupan dan keefektifan pengendalian yang ada di sistem. Jika hasil ujicoba menunjukkan bahwa sistem/ aplikasi telah sesuai dengan kebutuhan pengguna, maka harus dibuat suatu berita acara UAT yang disetujui pengguna.

2.4.2.6. Tahap Implementasi

Pada tahap ini hal-hal utama yang perlu dilakukan antara lain pemberitahuan jadwal implementasi, pelatihan pada pengguna dan instalasi sistem aplikasi yang telah

disetujui ke dalam lingkungan produksi. Hal-hal penting lainnya yang harus diperhatikan antara lain:

- a. pengecekan integritas program berupa pengendalian yang memadai terhadap konversi dari *source code* ke *object code* yang akan diimplementasikan;
- b. migrasi data dari sistem lama ke sistem baru;
- c. pengecekan akurasi dan keamanan data hasil migrasi pada sistem baru;
- d. kemungkinan diberlakukannya *parallel run* antara sistem yang lama dengan yang baru, sampai dipastikan bahwa data pada sistem yang baru telah akurat dan handal;
- e. integritas data, di mana Bank harus memastikan keakuratan dan kehandalan dari *database* dan integritas data;
- f. pada saat implementasi, *patching data* dapat sangat mempengaruhi integritas data pada *database* di server produksi, untuk itu harus dihindarkan;
- g. pengaturan penyimpanan *source code* dan *database* dari sistem lama.

2.4.2.7. Kaji Ulang Pasca Impelementasi (*Post Implementation Review*)

Manajemen harus melakukan *review* setelah implementasi pada akhir proyek untuk mengetahui bahwa seluruh aktivitas dalam proyek telah dilaksanakan dan tujuan proyek telah tercapai.

Manajemen harus menganalisa keefektifan aktivitas manajemen proyek dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek. Hasil analisa harus didokumentasikan dan dilaporkan kepada manajemen.

2.4.2.8. Tahap Pemeliharaan

Terhadap perangkat keras, perangkat lunak dan dokumentasi harus dilakukan pemeliharaan dalam rangka memastikan efektivitas operasional sistem. Bank harus menetapkan metodologi pemeliharaan yang sesuai dengan karakteristik dan risiko tiap proyek dari sistem aplikasi yang ada.

2.4.2.9. Tahap Disposal

Setiap perangkat lunak hasil pengembangan/pengadaan 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 dalam SDLC yaitu tahap *disposal/termination*. Hal ini dilakukan untuk memastikan sistem yang paling akurat dan terkini yang digunakan dalam kegiatan operasional serta menghindari

penyalahgunaan oleh pihak tidak berwenang. Pengaturan lebih lanjut mengenai kebijakan *disposal* dijelaskan pada Bab III Operasional.

2.4.3. Pengendalian Risiko Pada Pengadaan

Dalam hal akan digunakan sistem aplikasi yang dibeli dari pihak lain (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. Sama seperti halnya mengembangkan sistem aplikasi sendiri, studi kelayakan proyek pengadaan harus mendapat persetujuan manajemen, harus terdapat pendefinisian kebutuhan pengguna, harus memiliki pengendalian pengamanan yang memadai dan terdapat pengujian dan implementasi produk. Proses yang sama juga diterapkan dalam pengadaan perangkat keras dan perangkat lunak lainnya.

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 memperhatikan ketentuan terkait dan pedoman Bank Indonesia tentang *outsourcing*, serta ketentuan intern Bank. Selain itu Bank harus melakukan kaji ulang kontrak dan perjanjian lisensi (*licensing agreement*) untuk memastikan hak dan tanggung jawab masing-masing pihak jelas dan wajar. Penasehat hukum Bank harus melakukan konfirmasi bahwa jaminan pelaksanaan (*performance guarantees*), akses terhadap *source code*, masalah hak cipta, dan keamanan perangkat lunak/data telah diatur secara jelas sebelum pihak manajemen menandatangani kontrak.

2.4.3.1. Standar Pengadaan

Standar pengadaan harus diterapkan untuk memastikan bahwa produk yang dibeli telah memenuhi kebutuhan fungsional, kriteria keamanan, dan kehandalan. Alat utama dalam mengatur proyek pengadaan adalah *request for proposal* (RFP) yang sekurang-kurangnya memuat kebutuhan fungsional, keamanan, dan kebutuhan operasional secara tepat, jelas dan terperinci. Dalam pengadaan sistem, manajer proyek harus melakukan antara lain:

- a. meninjau ulang secara menyeluruh mengenai kesesuaian vendor, kontrak, lisensi dan produk yang diperoleh terhadap sistem yang ada.
- a. harus membandingkan penawaran dengan persyaratan yang ada dalam proyek dan antar sesama penawaran.
- b. mengkaji kondisi keuangan vendor dan komitmennya terhadap pelayanan.
- c. meminta pendapat penasehat hukum sebelum kontrak ditandatangani oleh manajemen.

2.4.3.2. Pedoman Proyek Pengadaan

Hal-hal yang harus diperhatikan dalam proyek pengadaan antara lain:

- a. proyek pengadaan dimulai dengan pengajuan rencana proyek kepada manajemen.
- b. prosedur harus ada untuk memfasilitasi proses permintaan dan memastikan manajemen *mereview* secara sistematis terhadap seluruh permintaan.
- c. permintaan harus didasarkan pada kebutuhan bisnis Bank untuk :
 - 1) mendapatkan suatu produk;
 - 2) mengidentifikasi fitur sistem yang diinginkan; dan
 - 3) menggambarkan kebutuhan informasi, *network interface*, komponen perangkat keras dan perangkat lunak.
- d. Bank harus menyusun studi kelayakan untuk menentukan apakah Bank membutuhkan pengadaan perangkat lunak baik yang dapat dimodifikasi sesuai kebutuhan atau siap pakai (*off-the shelf*).
- e. persetujuan dari seluruh pihak terkait atas studi kelayakan tersebut harus didokumentasikan untuk selanjutnya dapat menjadi dasar dibuatnya suatu definisi kebutuhan (*Requirement Definition*) seperti yang telah dijelaskan pada sub bagian 2.3.2.2 di atas.
- f. setelah Bank menerima penawaran, Bank harus menganalisa dan membandingkan penawaran antar peserta 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 Bank telah melakukan kaji ulang penawaran dengan benar. Proses seleksi akan menghasilkan daftar vendor potensial.
- h. manajemen harus mengkaji kembali kestabilan kondisi keuangan dan komitmen pelayanan dari vendor yang terpilih.
- i. Bank menentukan produk dan vendor serta menegosiasikan kontrak. Dalam hal ini penasehat hukum hendaknya meninjau ulang kontrak tersebut sebelum ditandatangani.

2.4.3.3. Escrow Agreement

Dalam hal aplikasi inti dibuat oleh pihak lain (*vendor*) dan *source code* tidak diberikan, kepentingan Bank dalam rangka menjaga kelangsungan usaha perlu dilindungi. Untuk memitigasi risiko atas terhentinya dukungan vendor maka Bank wajib mempertimbangkan perlu tidaknya memiliki perjanjian tertulis berupa *escrow agreement* atas perangkat lunak yang dianggap penting oleh Bank. Hal-hal yang dipertimbangkan dalam penggunaan *escrow agreement* antara lain reputasi *vendor*, perangkat lunak digunakan oleh banyak pihak baik di dalam maupun luar negeri.

Dalam *escrow agreement* terdapat pihak ketiga independen yang ditunjuk untuk menyimpan *source code*. Bank secara periodik (minimal per tahun) harus

memastikan bahwa pihak ketiga menyimpan versi terkini dari *source code*. Agen penyimpanan yang dipilih harus memastikan nomor dan tanggal versi *source* yang disimpan dan memastikan kepada vendor mengenai integritas dari *source code* tersebut.

2.4.3.4 . Kontrak Pengembangan dan Perjanjian Lisensi dari Perangkat Lunak

a. Lisensi Perangkat Lunak – Umum

Bank harus memastikan bahwa pada lisensi antara lain :

- 1) jelas tertulis apakah penggunaan perangkat lunak tersebut bersifat eksklusif atau tidak;
- 2) siapa dan berapa banyak personil pada Bank yang dapat menggunakan perangkat lunak termasuk penggunaan dalam jaringan;
- 3) apakah terdapat pembatasan lokasi penggunaan;
- 4) jika Bank menginginkan lisensi lokasi untuk pengguna yang tidak terbatas pada suatu lokasi, harus dipastikan bahwa di dalam kontrak hal tersebut dimungkinkan;
- 5) jika Bank menginginkan entitas terkait lainnya untuk menggunakan perangkat lunak tersebut, seperti *subsidiary* atau vendor harus terdapat dalam daftar lisensi.

Bank harus memastikan lisensi juga berlaku atas salinan *back-up* dari semua perangkat lunak penting yang dibutuhkan di tempat yang terpisah (*remote site*) dalam pelaksanaan *disaster recovery* atau memastikan kesinambungan kegiatan usaha Bank (*business continuity plan*). Bank harus memahami dengan jelas mengenai jangka waktu lisensi dan jika Bank menginginkan lisensi terus menerus untuk menggunakan perangkat lunak, harus dipastikan bahwa pada kontrak tertulis secara eksplisit mengenai hal tersebut.

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 perangkat dan infrastruktur yang dibutuhkan untuk menjalankan perangkat;
- 3) identifikasi dan spesifikasi fungsional di mana 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 pihak pengembang jika perangkat lunak gagal pada saat uji coba.

c. Pemeliharaan

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

- 1) vendor memberikan dokumentasi perangkat lunak, termasuk dokumentasi sistem aplikasi dan petunjuk teknis penggunaan;
- 2) pelaksanaan dan biaya dari pengkinian dan modifikasi perangkat lunak;
- 3) kemungkinan Bank melakukan akses ke *source code* bila pihak penyedia jasa tidak dapat memberikan layanan lagi atau terdapat modifikasi yang tidak dapat dilakukan oleh pihak penyedia jasa;
- 4) kemungkinan konversi perangkat lunak dan data ke perangkat lunak dan format data yang berbeda di masa mendatang.

Apabila diperlukan, hal-hal diatas dapat dimuat dalam suatu perjanjian pemeliharaan yang tersendiri.

d. Garansi

Penelitian perlu dilakukan Bank untuk meyakini bahwa lisensi perangkat lunak dari pihak vendor menjamin bahwa perangkat lunak:

- 1) tidak melanggar hak kekayaan intelektual dari pihak lainnya di seluruh dunia
- 2) tidak mengandung kode rahasia/ terbatas yang tidak diungkapkan atau pembatasan secara otomatis pada perjanjian
- 3) akan bekerja sesuai spesifikasi dan harus dinyatakan tanggung jawab vendor jika terjadi permasalahan
- 4) dijamin pemeliharaannya oleh vendor selama yang diperjanjikan
- 5) perjanjian lisensi tetap berlaku apabila terjadi merger, pengadaan atau perubahan kepemilikan baik pada Bank atau vendor.

e. Penyelesaian Perselisihan

Bank harus memasukkan klausula penyelesaian perselisihan pada kontrak dan 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.

f. 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.

g. Keamanan

Bank harus menetapkan kriteria pengendalian keamanan (*security control*) atas sistem Teknologi Informasi 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 harus membahas:

- 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) garansi dari vendor bahwa perangkat lunak tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam sistem aplikasi dan data Bank.
- 4) secara eksplisit menyatakan bahwa vendor tidak akan menggunakan fitur perangkat lunak yang dapat mengakibatkan perangkat lunak tersebut tidak berfungsi dengan baik.

h. Sub Kontrak Kepada Vendor Lain

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 di subkontrakkan maka harus terdapat persetujuan tertulis dari Bank. Dalam memberikan persetujuan sub kontrak tersebut, Bank harus mempertimbangkan tingkat kesulitan dan ketersediaan ahli dalam pengembangan perangkat lunak tersebut serta keamanan data Bank. Disamping itu Bank harus memastikan bahwa terdapat klausula bahwa vendor bertanggung jawab terhadap perangkat lunak meskipun dirancang atau dikembangkan oleh pihak lain.

2.4.4. Pengendalian Risiko Pada Pemeliharaan Sistem Aplikasi

Aktivitas pemeliharaan harus dilakukan oleh Bank mencakup layanan rutin dan modifikasi terhadap perangkat keras, perangkat lunak dan informasi yang terkait untuk memastikan efektifitas penggunaan Teknologi Informasi Bank. Untuk ini diperlukan Standar Operasional Prosedur tentang Manajemen Perubahan (*change management*) guna memastikan perubahan yang terjadi selama tahap pemeliharaan tidak akan mengganggu kegiatan operasional Teknologi Informasi Bank atau menurunkan kinerja/keamanan sistem. Manajemen perubahan mencakup modifikasi secara keseluruhan, modifikasi minor (kecil), dan perubahan yang bersifat mendesak (modifikasi darurat).

2.4.4.1. Manajemen Perubahan (*Change Management*)

Manajemen harus menetapkan SOP pengendalian perubahan secara detail yang memuat prosedur otorisasi, uji coba, dokumentasi, implementasi dan sosialisasi atas modifikasi teknologi tersebut.

Modifikasi mencakup perangkat keras dan lunak. Modifikasi perangkat keras dibutuhkan untuk menggantikan peralatan yang lama atau tidak berfungsi atau bahkan untuk meningkatkan kinerja atau kapasitas penyimpanan. Modifikasi perangkat lunak dibutuhkan untuk memenuhi kebutuhan pengguna, memperbaiki permasalahan perangkat lunak dan kelemahan keamanan atau mengimplementasikan teknologi baru. Bank harus mengkoordinasikan modifikasi perangkat lunak dan *patch* melalui proses manajemen perubahan yang terpusat karena adanya keterkaitan antar sistem aplikasi dan sistem operasional.

Berdasarkan tingkat kepentingannya, modifikasi digolongkan menjadi:

- 1) modifikasi utama (*major modification*), merupakan perubahan fungsional secara signifikan pada sistem aplikasi yang antara lain disebabkan karena adanya konversi atau pengembangan sistem baru akibat adanya merger atau akuisisi Bank. Modifikasi utama harus diterapkan mengikuti proses yang terstruktur seperti yang dilakukan dalam siklus pengembangan sistem/aplikasi.
- 2) modifikasi minor, merupakan pelaksanaan perubahan pada sistem aplikasi atau perangkat lunak sistem operasi untuk meningkatkan kinerja, memperbaiki permasalahan atau meningkatkan keamanan. Standar modifikasi minor harus mencakup permintaan perubahan, peninjauan kembali dan prosedur persetujuan serta mensyaratkan manajemen untuk merencanakan, menguji coba dan mendokumentasikan semua perubahan sebelum dilakukan implementasi. Bank harus melakukan kaji ulang semua modifikasi yang diusulkan untuk memastikan kesesuaian modifikasi dengan sistem yang ada dan memastikan bahwa hanya modifikasi yang disetujui yang diimplementasikan. Bank harus menetapkan standar persetujuan program yang mencakup prosedur untuk memverifikasi hasil uji coba, memeriksa kode yang diubah dan memastikan kesesuaian *source code*. . Setelah modifikasi program selesai, semua *source code* harus diamankan dalam *library* baik versi terkini maupun versi sebelum diubah.
- 3) modifikasi darurat, dibutuhkan untuk memperbaiki permasalahan pada perangkat lunak atau mengembalikan proses operasional dengan cepat. Meskipun modifikasi tersebut harus diselesaikan dengan cepat, namun tetap harus diimplementasikan dan dikendalikan dengan baik. Sebagaimana layaknya modifikasi, modifikasi darurat harus diuji sebelum implementasi. Namun jika uji coba tidak dapat dilakukan secara menyeluruh pada modifikasi darurat sebelum implementasi, harus ada prosedur untuk melakukan *backup file* dengan benar. Hal ini penting agar Bank dapat membatalkan modifikasi jika modifikasi tersebut menyebabkan gangguan pada sistem.

2.4.4.2. Patch Management

Vendor secara rutin mengembangkan dan mengeluarkan *patches* untuk memperbaiki permasalahan pada perangkat lunak, memperbaiki kinerja, dan meningkatkan keamanan. Jika terdapat *patch* baru, Bank harus mengevaluasi dampak secara teknis dari instalasi *patch* tersebut terhadap bisnis dan *security*. Bank harus memiliki prosedur untuk mengidentifikasi ketersediaan *patches* dari sumber yang terpercaya. Standar pengaturan *patch* harus mencakup prosedur identifikasi, evaluasi, persetujuan, pengujian, instalasi, dan dokumentasi dari *patches*. Bank harus meninjau ulang semua *security setting* dan *configuration parameter* setelah penggunaan *patch* baru untuk memastikan bahwa *setting* telah memenuhi kebijakan dan prosedur yang disetujui.

2.4.4.3. Library

Untuk memastikan ketersediaan program yang digunakan, Bank harus memiliki *Library* untuk menyimpan program. Selain itu perlu disimpan juga informasi dan atau dokumen berupa data dan program yang berhubungan dengan server/mesin produksi yang berasal dari pengembangan dan atau pengujian. Pengaturan lebih lanjut mengenai pengendalian terhadap *library* dijelaskan pada Bab III - Operasional.

2.4.4.4. Konversi

Apabila terjadi merger Bank atau akuisisi yang memerlukan pengintegrasian sistem yang digunakan Bank yang terlibat dalam merger atau akuisisi, maka perlu dilakukan proses konversi. Dalam proses ini dilakukan modifikasi besar pada sistem aplikasi atau sistem operasi yang ada dan pengembangan sistem baru apabila diperlukan. Dalam proses konversi ini, proses yang terstruktur seperti siklus pengembangan sistem/aplikasi tetap harus diterapkan.

Mengingat kompleksitas sistem di masing-masing Bank yang terlibat merger, 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 (*help desk*), penyelesaian masalah (*troubleshooting*), keterhubungan jaringan dan sistem administrasi.

2.4.4.5. Pemeliharaan Dokumentasi

Standar dokumentasi harus mengidentifikasi dokumen utama dan dokumen detail yang telah disetujui dan sesuai format yang diinginkan. Dokumentasi tersebut harus berisi semua perubahan yang terjadi pada sistem, aplikasi dan konfigurasi sesuai dengan standar yang ditentukan.

BAB III

AKTIVITAS OPERASIONAL TEKNOLOGI INFORMASI

3.1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) memungkinkan bank menjalankan kegiatan operasional yang semakin kompleks. Operasional TI tidak hanya terkonsentrasi di pusat data (*Data Center*) tetapi juga pada aktivitas lainnya 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 *user* dari berbagai lokasi. Demikian juga dengan pemrosesan, dapat dilakukan di berbagai lokasi yang berjauhan namun saling terkait, baik secara *online realtime*, *on-line*, maupun *off-line*. Oleh karena itu diperlukan pengendalian yang memadai atas operasional TI agar bank dapat meminimalisasi risiko terganggunya kerahasiaan, integritas, dan ketersediaan informasi.

Bab ini membahas aktivitas, risiko, dan pengendalian dari operasional TI yang dapat dijadikan pedoman bagi Bank dalam rangka menerapkan manajemen risiko dalam penggunaan TI di Bank. Pengaturan atas aktivitas operasional TI yang memadai sangat penting untuk memastikan informasi pada sistem komputer adalah lengkap, akurat, terkini, terjaga integritasnya, dan handal, serta terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan, dan perusakan data.

3.2. TUGAS DAN TANGGUNG JAWAB MANAJEMEN

Manajemen Bank bertanggung jawab untuk memastikan mekanisme operasional TI yang stabil, aman, dan efisien secara keseluruhan, baik yang diselenggarakan sendiri maupun menggunakan jasa pihak lain. Manajemen harus menetapkan kebijakan, standar, dan prosedur operasional TI yang menjamin kesinambungan operasional TI Bank dan memastikan penerapannya baik pada satuan kerja penyelenggara TI atau pihak penyedia jasa maupun pada satuan kerja pengguna TI. Kesalahan atau kegagalan yang terjadi pada aktivitas operasional TI dapat mengganggu kegiatan operasional dan pelayanan bank kepada nasabah yang pada akhirnya mempengaruhi reputasi bank. Oleh karena itu manajemen harus memastikan penilaian risiko dilakukan secara berkala pada aktivitas operasional TI dan memutuskan penanganan risiko potensial yang tepat sesuai dengan *risk appetite* yang telah ditetapkan.

3.3. KEBIJAKAN DAN PROSEDUR

Bank wajib memiliki kebijakan yang mencakup setiap aspek operasional TI. Kedalaman dan cakupan kebijakan tersebut disesuaikan dengan kompleksitas operasional TI Bank.

Kebijakan harus dijabarkan dalam prosedur tertulis yang digunakan dalam pelaksanaan operasional TI. Prosedur memuat tanggung jawab, akuntabilitas, pemberian wewenang, pedoman bagi para pelaksana. Selain itu manajemen harus menetapkan standar, yaitu persyaratan yang harus dipenuhi oleh perangkat keras dan perangkat lunak yang dipergunakan di lingkungan produksi, pengujian, dan pengembangan dalam penyelenggaraan TI Bank.

3.3.1. Kebijakan Operasional *Data Center*

Kebijakan, sistem dan prosedur serta standar yang diterapkan dalam aktivitas operasional *Data Center* mencakup aktivitas menjalankan tugas rutin maupun non-rutin. Aktivitas yang terkait dengan operasional *Data Center* antara lain:

- a. penjadwalan tugas:
Bank wajib memiliki dan melaksanakan jadwal semua tugas yang harus dijalankan di *Data Center* operasional TI efektif dan aman dari perubahan yang tidak sah.
- b. pengoperasian tugas:
pemberian akses *command line* kepada operator TI harus dibatasi sesuai kewenangan pada fungsi pengoperasian tugas yang telah ditentukan.
- c. pendistribusian laporan/*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 *logik* dan pemusnahan *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, dan untuk dapat memastikan keamanan *output*.
- d. proses *backup* baik *on-site* maupun *off-site*, *restore*, *download* dan *upload* untuk *data/database*;
- e. pengaktifan jejak audit (*audit trail*).

3.3.2. Kebijakan Perencanaan Kapasitas

Bank perlu memiliki kebijakan dan prosedur perencanaan kapasitas 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 yang baik, Bank dapat menghadapi risiko kekurangan atau bahkan pemborosan sumber daya TI. Perencanaan kapasitas hendaknya disusun untuk jangka waktu cukup panjang dan selalu dikinikan untuk mengakomodir perubahan yang ada.

3.3.3. 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;
- c. inventarisasi dan pengkinian informasi perangkat keras dan perangkat lunak, perangkat jaringan, media penyimpanan dan perangkat pendukung lainnya yang terdapat di *Data Center*.

Inventarisasi yang dilakukan meliputi hal-hal sebagai berikut:

- a. perangkat keras:

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

Bank harus melakukan inventarisasi atas informasi mengenai nama dan jenis perangkat lunak (sistem operasi, sistem aplikasi, atau sistem utilitas). Informasi lain yang harus dicakup dalam inventarisasi perangkat lunak meliputi nama pembuat atau *vendor*, tanggal instalasi, nomor versi dan keluaran (*release*), pemilik perangkat lunak, *setting* parameter dan *service* yang aktif, jumlah lisensi yang dimiliki, jumlah yang di-*install* dan jumlah *user*.
- c. perangkat jaringan:

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

 - 1) diagram jaringan;
 - 2) identifikasi seluruh koneksi intern dan ekstern Bank;
 - 3) daftar dan kapasitas peralatan jaringan seperti *switch*, *router*, *hub*, *gateway*, *firewall*, dll;
 - 4) identifikasi vendor telekomunikasi antara intern Bank, Bank dengan pihak lain, dan dengan internet;
 - 5) rencana perluasan dan perubahan konfigurasi jaringan;
 - 6) gambaran sistem pengamanan jaringan.
- d. media penyimpan:

informasi yang diperlukan dalam inventarisasi media penyimpan antara lain jenis dan kapasitas, lokasi penyimpanan baik *on-site* maupun *off-site*, tipe dan klasifikasi data yang disimpan, *source system* serta frekuensi dan masa retensi *backup*.
- e. perangkat pendukung *Data Center*

Bank harus menginventarisasi perangkat pendukung *Data Center* antara lain UPS dan *power control, fire detection and extinguisher, air conditioning*, pengukur suhu dan kelembaban udara.

3.3.4. Kebijakan Pemeliharaan Perangkat Keras dan Perangkat Lunak

3.3.4.1. Perawatan Perangkat Keras dan Fasilitas *Data Center*

Perawatan preventif secara berkala terhadap peralatan TI perlu dilakukan untuk meminimalkan kegagalan pengoperasian peralatan tersebut dan untuk mendeteksi secara dini permasalahan yang potensial. Untuk itu bank perlu memiliki kontrak perawatan dengan *vendor* guna memastikan ketersediaan dukungan perawatan dari *vendor*. Semua perawatan yang dilakukan hendaknya didasarkan jadwal yang telah ditetapkan, di dokumentasikan pada suatu *log* dan dilakukan *review* secara berkala.

3.3.4.2. Pengamanan Fisik dan Pengendalian Lingkungan *Data Center*

a. Pengendalian Akses Fisik Pusat Data (*Data Center*):

Akses fisik ke *Data Center* harus dibatasi dan dikendalikan dengan baik. Pintu *Data Center* harus selalu terkunci, dilengkapi dengan kartu akses dan atau *biometric device*. Ruang *Data Center* tidak boleh diberi label atau papan petunjuk (*signing board*) sehingga orang mudah mengenalinya. Bank harus memiliki *log-book* untuk mencatat tamu yang memasuki *Data Center*.

b. Pengendalian Lingkungan Pusat Data:

Kondisi lingkungan pemrosesan TI yang tidak sesuai standar dapat menimbulkan gangguan pada operasi TI. Oleh karenanya, manajemen harus melakukan antara lain:

- 1) mengawasi dan memantau faktor lingkungan *data center*, antara lain mencakup: sumber listrik, api, air, suhu, kelembaban udara. Pengendalian lingkungan yang dapat diterapkan antara lain: penggunaan UPS (*Uninterruptible Power Supply*), *raised floor* (lantai yang ditinggikan), pengaturan suhu dan kelembaban udara (AC, termometer, dan hidrometer), pendeteksi asap/api/panas, sistem pemadaman api, dan kamera CCTV.
- 2) memastikan tersedianya sumber listrik yang cukup, stabil, dan tersedianya sumber alternatif 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*) jika terjadi gangguan pada salah satu sumber listrik untuk menjaga pasokan listrik yang sesuai dengan kebutuhan peralatan.

- 3) memastikan *Data Center* memiliki detektor api dan asap serta pipa pembuangan air. Selanjutnya, Bank 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 *Data Center*.
 - 4) menggunakan lantai yang ditinggikan (*raised floor*) untuk mengamankan sistem perkabelan dan menghindari efek *grounding* di *Data Center*.
- c. Kinerja Perangkat Keras dan Perangkat Lunak:
- Pemantauan terhadap perangkat keras dan perangkat lunak minimal dilakukan setiap hari untuk memastikan seluruh perangkat tersebut beroperasi sebagaimana mestinya, misalnya *server* tetap dalam keadaan menyala, kapasitas *database* dan utilitas *server* tidak melampaui limit, dan fasilitas pendukung berfungsi dengan baik.

3.3.5. Kebijakan Pengelolaan Perubahan (*Change Management*)

Change Management adalah prosedur yang mengatur penambahan, penggantian, maupun penghapusan obyek di lingkungan produksi. Obyek dimaksud dapat berupa data, program, menu, aplikasi, perangkat komputer, perangkat jaringan, dan proses. Bank harus memiliki kebijakan dan prosedur *Change Management* yang paling kurang mencakup permintaan, analisis, dan persetujuan perubahan dan instalasi perubahan termasuk pemindahan perangkat keras dan perangkat lunak dari lingkungan pengujian ke lingkungan produksi.

Change Management harus memperhatikan hal-hal sebagai berikut:

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 *Change Management* yang terkoordinir dan melibatkan perwakilan dari satuan kerja bisnis, unit penyelenggara TI, keamanan informasi, dan audit internal. Prosedur instalasi perubahan harus memperhatikan kelangsungan operasional pada lingkungan produksi, pengawasan, dan pengaturan pengamanan sistem informasi. Standar minimum yang diatur harus mencakup risiko, pengujian, otorisasi dan persetujuan, waktu implementasi, validasi setelah penginstalan dan *back-out* atau *recovery*.

b. *Patch Management*:

Dalam *Change Management*, Bank harus memiliki dokumentasi yang lengkap tentang instalasi *patch* yang dilakukan. Selain itu Bank harus memastikan bahwa Bank menggunakan versi perangkat lunak dengan *release* 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 bank, atau terjadi penggabungan data dari beberapa sistem yang berbeda. Dalam hal terdapat migrasi data, Bank perlu memiliki kebijakan, prosedur mengenai penanganan migrasi data. Tahap-tahap yang perlu dilalui dalam melakukan migrasi data dimulai dari rencana strategis, manajemen proyek, *Change Management*, pengujian, rencana kontinjensi, *back-up*, manajemen vendor, dan *post implementation review*.

3.3.6. Kebijakan Penanganan Kejadian/Permasalahan

Tanpa prosedur penanganan kejadian/permasalahan yang baik, Bank dapat menghadapi risiko finansial, operasional, dan reputasi dari permasalahan yang timbul. Prosedur penanganan kejadian/permasalahan harus mencakup perangkat keras, sistem operasi, sistem aplikasi, perangkat jaringan, dan peralatan keamanan. Penjelasan lebih lanjut dapat dilihat pada Bab V Pengamanan Informasi - Penanganan Insiden dalam Pengamanan Informasi.

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

a. *Help Desk*

Fungsi help desk harus dimiliki oleh Bank agar Bank cepat tanggap terhadap permasalahan yang dihadapi oleh seluruh pengguna (*user*) di Bank dan menanganinya segera. Bank akan menghadapi risiko jika tidak memiliki prosedur *helpdesk* yang memadai yaitu tidak dapat dipastikannya bahwa pengguna senantiasa memiliki tempat bertanya dan memperoleh jawaban dan solusi atas permasalahan-permasalahan yang dihadapi.

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

1) Tersedianya dokumentasi permasalahan yang lengkap.

Dokumentasi permasalahan harus mencakup data user, 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* yang berbasis pengetahuan.

Bank perlu menggunakan sistem yang berbasis pengetahuan untuk memberikan dukungan 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. Penanganan penggunaan *Power User*

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

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

3.3.7. Kebijakan Pengelolaan *Data Warehouse* (DWH)

Bank harus memiliki kebijakan dan prosedur tentang pengendalian terhadap DWH. Pengendalian terhadap sistem yang digunakan untuk DWH pada dasarnya diperlakukan sama dengan pengendalian yang diterapkan terhadap sistem *core banking* dan sistem lain yang merupakan sumber data bagi DWH. Jika pada sistem aplikasi sumber, data tersebut diperlakukan sebagai data rahasia dan aksesnya terbatas, maka pada DWH juga harus diperlakukan demikian juga. Pembatasan akses ini tidak terbatas pada akses *logical* tetapi juga akses secara fisik terhadap sarana pendukung DWH dan laporan-laporan yang dihasilkannya. Adapun yang dimaksud dengan sistem mencakup sistem operasi, sistem aplikasi, dan sistem jaringan.

3.3.8. Kebijakan Pengelolaan *Database*

Kegagalan dalam mengelola dan mengamankan *database* secara tepat dapat mengakibatkan perubahan, penghancuran, atau pengungkapan informasi yang sensitif oleh *user* secara sengaja maupun tidak sengaja atau oleh pihak lain yang tidak berhak. Pengungkapan tanpa ijin terhadap informasi yang rahasia dapat mengakibatkan risiko reputasi, hukum, dan operasional dan dapat menyebabkan kerugian finansial. Bank perlu memiliki klasifikasi sensitivitas atas informasi yang disimpan pada *database* sebagai dasar untuk melakukan pengawasan. *Database* yang menyimpan informasi rahasia membutuhkan pengendalian yang lebih ketat dibandingkan *database* yang menyimpan informasi yang tidak sensitif. Untuk itu, Bank wajib memiliki fungsi *Database Administrator* (DBA) yang bertanggung jawab terhadap pengelolaan *database* bank.

Prosedur yang wajib dimiliki Bank terkait *database* adalah pengaksesan, pemeliharaan, penanganan permasalahan dan administrasi *database*.

3.3.9. Kebijakan Pengendalian Pertukaran Informasi (*Exchange of Information*)

Pengiriman informasi secara *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 *logik* antara lain:

- a. permintaan dan pemberian informasi oleh pihak internal dan eksternal;
- b. pengiriman informasi melalui berbagai media, seperti: *hardcopy*, *tape*, *disk*, *e-mail*, *pos*, dan *internet*.

Pada bank besar dengan kompleksitas TI yang tinggi, manajemen harus mempertimbangkan pemisahan segmen WAN dan LAN dengan perangkat pengamanan (seperti *firewall*) yang membatasi akses dan lalu lintas keluar masuknya data.

3.3.10 Kebijakan Fungsi *Library*

Fungsi *librarian* bertanggung jawab untuk menginventarisir dan menyimpan seluruh perangkat lunak dan data yang tersimpan dalam berbagai media, antara lain *tape* dan *disk*. Disamping itu *librarian* juga menyimpan *copy* dari seluruh kebijakan dan prosedur seperti *Data Center run book manual*.

Adapun prosedur yang harus ditetapkan antara lain:

- a. pengamanan akses ke data di *library*;
- b. penanganan media penyimpan data (untuk data/*database* dan *audit journal*);
- c. masa retensi media penyimpan data;
- d. pengetesan media penyimpan data;
- e. keluar dan masuk media penyimpan data dari dan ke *library*;

Dalam membuat kebijakan dan prosedur serta standar untuk *library*, Bank harus memperhatikan kecukupan prosedur penyimpanan (*storage*)/*back-up* dan pembuangan (*disposal*) media. *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.

3.3.10 Kebijakan Fungsi *Quality Assurance* (QA)

Setiap pembuatan dan perubahan sistem harus melalui persetujuan fungsi QA sebelum dipindahkan (migrasi) ke lingkungan produksi sesuai dengan pedoman pengembangan sistem dan *change management*. Fungsi QA melakukan penilaian kualitas perangkat keras dan perangkat lunak sesuai dengan standar yang ditetapkan.

3.3.11. Kebijakan Pengelolaan Hubungan dengan Pihak Penyedia Jasa

Apabila TI yang digunakan oleh Bank diselenggarakan oleh pihak lain maka Bank wajib memantau dan mengevaluasi kehandalan pihak penyedia jasa secara berkala baik yang menyangkut kinerja, reputasi penyedia jasa dan kelangsungan penyediaan layanan. Untuk itu, Bank harus menunjuk personil yang bertugas memantau layanan

penyedia jasa TI dengan menggunakan prosedur yang paling kurang mencakup pemantauan layanan, pelaporan permasalahan dan dokumentasi yang terkait dengan layanan pihak penyedia jasa.

3.3.12. Kebijakan Penghapusan Perangkat Keras dan Perangkat Lunak (*Disposal*)

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

- a. memindahkan data dari sistem produksi ke media *backup* dengan mekanisme sesuai prosedur, termasuk prosedur uji coba dan *backup*;
- b. menyimpan dokumentasi sistem sebagai persiapan jika diperlukan untuk meng-*install* ulang suatu sistem ke server produksi;
- c. mengelola arsip data sesuai masa retensi;
- d. menghancurkan data yang habis masa retensinya.

3.4. MANAJEMEN RISIKO OPERASIONAL TI

Proses manajemen risiko adalah mengidentifikasi, mengukur, mengendalikan, dan memantau risiko pada fungsi-fungsi yang terkait dengan operasional TI.

3.4.1. Identifikasi Risiko Operasional TI

Proses identifikasi dimulai dengan pemahaman yang komprehensif terhadap bagaimana Bank mengoperasikan TI demi mendukung tujuan organisasi kemudian mengidentifikasi risiko yang dihadapi Bank. Manajemen harus memperhatikan kejadian atau aktivitas yang dapat mengganggu operasional antara lain hal-hal berikut ini:

- a. Kesalahan investasi teknologi termasuk penerapan yang tidak benar, kegagalan dari pihak supplier, pendefinisian dari kebutuhan bisnis yang tidak tepat, ketidaksesuaian dengan sistem-sistem yang ada, atau keusangan *software* (termasuk hilangnya dukungan *vendor* terhadap perangkat keras dan perangkat lunak yang digunakan oleh Bank);
- b. 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;
- c. Permasalahan pada kapasitas sistem seperti kekurangan pada perencanaan kapasitas, ketidakcukupan kapasitas untuk mengakomodasi fleksibilitas sistem, ketidakcukupan *software* untuk mengakomodasi pengembangan bisnis;

- d. Kegagalan sistem termasuk pada jaringan, *interface*, perangkat keras, perangkat lunak, atau kegagalan komunikasi internal; dan
- e. Pelanggaran pada keamanan sistem termasuk pelanggaran pada keamanan eksternal dan internal, penipuan dalam pemrograman, atau virus pada komputer.

3.4.2. Pengukuran Risiko Operasional TI

Tinggi rendahnya risiko yang diukur tergantung pada faktor-faktor yang terkait antara lain terdiri dari:

- a. tingkat kepentingan bisnis;
- b. perubahan pada cakupan sistem atau proses;
- c. lokasi pengaksesan sistem (internal atau eksternal, termasuk *internet*, *dial-up*, atau WAN);
- d. sumber aplikasi: beli paket, dikembangkan secara internal, atau kombinasi dari keduanya;
- e. cakupan dan tingkat kekritisitas sistem atau banyaknya unit bisnis yang terpengaruh;
- f. kompleksitas tipe pemrosesan (*batch*, *real-time*, *client/server*, *parallel distributed*);
- g. volume transaksi dan nilai transaksi;
- h. klasifikasi dan sensitivitas data yang diproses atau digunakan;
- i. dampak pada data (*read*, *download*, *upload*, *update* atau *alter*);
- j. tingkat pengalaman dan kemampuan pengelola TI;
- k. kecukupan jumlah dan kemampuan staf pelaksana;
- l. keragaman *platform*, aplikasi dan *delivery channel*;
- m. jumlah pengguna dan nasabah;
- n. perubahan regulasi;
- o. adanya risiko yang baru atau sedang berkembang dari teknologi yang sedang dikembangkan atau risiko keusangan teknologi; dan
- p. adanya kelemahan audit atau kelemahan yang ditemui dalam *self-assessment*.

3.4.3. Pengendalian Risiko Operasional TI

Atas setiap fungsi operasi TI yang ada, Bank harus memitigasi risiko yang telah diidentifikasi dan diukur dengan cara-cara pengendalian yang telah ditetapkan dalam kebijakan dan prosedur operasional TI Bank. Meskipun telah dimitigasi, Bank harus tetap memantau risiko yang dikendalikan dan risiko sisa karena setiap gangguan yang terdapat pada operasional TI pada akhirnya berdampak pada risiko operasional, strategis, transaksi, dan reputasi Bank.

3.5. AUDIT INTERN

Audit atas operasional TI perlu dilakukan untuk memastikan proses manajemen risiko operasional TI berjalan dengan baik. Pengaturan lebih rinci mengenai audit intern di bahas pada Bab IX tentang Audit Intern TI.

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 berbagai produk perbankan secara *on-line realtime* dari seluruh kantor dan *delivery channel* lainnya, seperti; *Automated Teller Machine (ATM)*, *internet Banking*, *mobile Banking*, dan *Electronic Data Capture (EDC)*, baik milik Bank itu sendiri maupun milik pihak penyedia jasa.

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 terpengaruh adanya perubahan dan rentan terhadap gangguan dan penyalahgunaan. Oleh karena itu Bank perlu memastikan bahwa integritas jaringan dipelihara dengan cara menerapkan kebijakan 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. PERAN DAN TANGGUNG JAWAB MANAJEMEN

Keamanan jaringan komunikasi merupakan tanggung jawab seluruh pihak dalam Bank. Dalam pelaksanaannya Bank perlu memiliki petugas/fungsi yang menangani jaringan komunikasi. Petugas/fungsi tersebut harus melakukan koordinasi dengan fungsi pengelola pengamanan TI. Bank harus meyakini ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola oleh pihak internal Bank maupun pihak penyedia jasa, diantaranya dengan tersedianya cadangan peralatan dan jasa yang memadai. Manajemen harus memastikan terdapatnya pengawasan yang memadai dalam pengoperasian jaringan komunikasi dan pada setiap pengembangan atau modifikasi jaringan komunikasi. Manajemen perlu mempertimbangkan kebutuhan layanan yang diinginkan sesuai dengan kondisi bisnis saat ini dan strategi yang akan dikembangkan.

4.3. KEBIJAKAN DAN PROSEDUR

Bank harus memiliki kebijakan dan prosedur sebagai pedoman dalam menerapkan teknologi jaringan komunikasi untuk meyakinkan bahwa kelangsungan operasional dan keamanan jaringan komunikasi tetap terjaga. Untuk itu Bank wajib menetapkan *baseline/standar* yang digunakan secara internal untuk masing-masing.

platform (misal berdasarkan protokol atau sistem operasi) dan diterapkan di semua jaringan komunikasi yang digunakan oleh Bank.

Kebijakan dan prosedur yang perlu ditetapkan sekurang-kurangnya mencakup hal-hal sebagai berikut:

- a. pengukuran kinerja dan perencanaan kapasitas jaringan (*performance and capacity planning*);
- b. pengamanan jaringan komunikasi (*network access controls*, termasuk *remote access*);
- c. *change management (setting, configuration and testing)*;
- d. *network management, logging dan monitoring*;
- e. penggunaan *internet, intranet, e-mail* dan *wireless* (termasuk mekanisme penggunaan jaringan komunikasi);
- f. tersedianya prosedur penanganan masalah (*problem handling*);
- g. tersedianya fasilitas untuk *backup & recovery*;
- h. kecukupan kontrak dan tersedianya SLA yang sesuai dengan kebutuhan Bank dan dipantau secara berkala apabila jaringan komunikasi yang digunakan oleh Bank diselenggarakan oleh pihak penyedia jasa.

4.4. MANAJEMEN RISIKO JARINGAN KOMUNIKASI

Bank harus melakukan identifikasi kemungkinan yang akan terjadi, mengukur dampak yang mungkin ditimbulkan, dan melakukan upaya-upaya untuk mengelola risiko penggunaan jaringan komunikasi. Berdasarkan hasil pengukuran yang telah dilakukan atas risiko yang signifikan, maka Bank harus menerapkan pengendalian yang memadai. Bank juga harus senantiasa memantau apakah seluruh risiko yang signifikan tersebut telah ditangani dengan baik.

4.4.1. Identifikasi Risiko

Penggunaan teknologi jaringan komunikasi memberikan berbagai kemudahan dan manfaat bagi Bank dan nasabah, namun demikian, perlu diperhatikan risiko-risiko yang mungkin timbul, antara lain:

- a. kehilangan data/informasi;
- b. kehilangan integritas data/informasi;
- c. tidak lengkapnya data/informasi yang ditransmisikan;
- d. hilangnya kerahasiaan informasi;
- e. tidak tersedianya jaringan komunikasi akibat gangguan atau bencana;
- f. kehilangan/kerusakan perangkat jaringan komunikasi.

4.4.2. Pengendalian Risiko

Dalam mengendalikan risiko pada jaringan komunikasi, Bank harus memperhatikan hal-hal sebagai berikut:

a. Desain Jaringan Komunikasi

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

- 1) penentuan topologi jaringan komunikasi;
- 2) perencanaan kapasitas (*capacity planning*) jaringan komunikasi;
- 3) pemilihan media jaringan komunikasi;
- 4) *backup* perangkat keras, *alternative routing* (jalur alternatif) atau *provider* alternatif;
- 5) pengamanan fisik dan *logic*:
 - a) penempatan perangkat jaringan pada lokasi yang aman terhadap gangguan alam dan akses oleh orang yang tidak berhak;
 - b) pengaturan parameter sistem perangkat jaringan.
- 6) tersedianya jejak audit, sekurang-kurangnya terhadap perubahan-perubahan pada *setting* parameter dan hak akses perangkat jaringan komunikasi dan juga penggunaan atas hak akses tersebut.

b. 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:

- 1) akses ke jaringan komunikasi oleh *user* didasarkan pada kebutuhan bisnis dengan memperhatikan aspek keamanan informasi.
- 2) melakukan pemisahan jaringan komunikasi berdasarkan segmen baik secara *logical* maupun fisik, misalnya pemisahan antara lingkungan pengembangan dan produksi.
- 3) jika pemisahan secara fisik tidak dapat dilakukan, maka Bank harus memisahkan jaringan komunikasi secara *logical* dan memantau *security access* di jaringan komunikasi.
- 4) keputusan untuk terhubung ke jaringan komunikasi di luar Bank harus sesuai dengan persyaratan pengamanan dan secara formal disetujui oleh manajemen sebelum pelaksanaan.
- 5) menerapkan pengendalian yang dapat membatasi *network traffic* yang tidak sah atau tidak diharapkan.
- 6) konfigurasi perangkat jaringan komunikasi harus diset dengan baik. Fungsi-fungsi atau *services* yang tidak dibutuhkan harus dinonaktifkan.
- 7) penggunaan perangkat pengamanan jaringan komunikasi, seperti *firewall*, *Intrusion Detection System (IDS)*, dan *Intrusion Prevention System (IPS)*.

- 8) penggunaan penambahan perangkat monitor jaringan komunikasi (*network management system*) dengan memperhatikan pengamanannya.
 - 9) pengujian secara berkala terhadap keamanan jaringan komunikasi, misalnya dengan *penetration testing*.
- c. Operasi dan Pemeliharaan Jaringan Komunikasi
- Pengoperasian dan pemeliharaan jaringan komunikasi harus dilakukan dengan memperhatikan hal-hal berikut ini:
- 1) petugas yang mengoperasikan jaringan komunikasi harus secara jelas ditunjuk oleh manajemen, memiliki kemampuan pengetahuan dan keterampilan yang cukup, dan diberi tugas dan wewenang yang memadai untuk menjalankan fungsinya;
 - 2) Bank harus memiliki *incident response plan* terhadap gangguan dan serangan jaringan komunikasi;
 - 3) Bank harus memiliki fasilitas *backup* perangkat keras/lunak jaringan komunikasi, termasuk mekanisme *restart/recovery* yang telah teruji. Fasilitas *backup* tersebut sebaiknya memiliki risiko yang berbeda dengan perangkat utama seperti menggunakan pihak penyedia jasa yang berbeda;
 - 4) *patch* dan *release* harus selalu dikinikan (setelah melalui pengujian intern) untuk meyakini bahwa kelemahan-kelemahan telah diperbaiki.

4.4.3. Monitoring Risiko

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

- 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 yang diperlukan untuk rencana pengembangan bisnis dibandingkan dengan kapasitas terpasang;
- d. Bank harus memantau dan menindaklanjuti penyusupan/serangan terhadap jaringan komunikasi;
- e. Bank harus melakukan kaji ulang pemberian akses ke pengguna secara berkala untuk meyakinkan bahwa akses yang diberikan masih sesuai dengan tugas dan wewenangnya. Selain itu perlu dilakukan kaji ulang atas pengguna jaringan komunikasi di Bank yang memiliki akses ke jaringan komunikasi di luar Bank.

4.5. PENGENDALIAN INTERN

4.5.1. Audit Intern

Audit terhadap jaringan komunikasi harus dilakukan secara berkala oleh pihak independen, baik Auditor Intern maupun Auditor Ekstern. Ruang lingkup audit atas jaringan komunikasi antara lain mencakup kinerja jaringan komunikasi, *logical access*, *physical access*, *remote access*, infrastruktur jaringan komunikasi, dokumentasi jaringan komunikasi. Pengaturan lebih lengkap tentang audit mengacu pada **Bab X tentang Audit Intern TI**.

4.5.2. Dokumentasi

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

- a. kebijakan, prosedur, standar, 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 monitoring jaringan komunikasi;
- f. laporan perencanaan kapasitas jaringan komunikasi;
- g. kontrak dan SLA dengan pihak ketiga penyedia jasa fasilitas jaringan komunikasi;
- h. dokumen pengujian jaringan komunikasi;
- i. dokumen pengimplementasian jaringan komunikasi;
- j. dokumen perubahan jaringan komunikasi disertai alasannya;
- k. daftar *user* dan wewenangnya.

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 tersebut, namun juga nasabah, Bank lain dan bahkan terhadap sistem perbankan nasional. Mengingat pentingnya informasi, maka informasi harus dilindungi atau diamankan oleh seluruh personil di Bank. Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen TI terkait, seperti perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC) dan sumber daya manusia (termasuk kualifikasi dan ketrampilan).

5.2. TUGAS DAN TANGGUNG JAWAB

5.2.1. Dewan Komisaris

Dalam tugasnya mengarahkan dan melakukan evaluasi terhadap kebijakan Bank dalam pengelolaan pengamanan Teknologi Informasi Dewan Komisaris hendaknya melakukan koordinasi dengan direksi, antara lain meminta Direksi melaporkan pembagian wilayah wewenang dan tanggung-jawab pada satuan kerja penyelenggara TI dan satuan kerja pengguna TI, upaya peningkatan pengendalian pengamanan informasi, serta penentuan risiko sisa (*residual risk*) yang akan ditanggung Bank. Evaluasi tersebut mencakup juga evaluasi terhadap dampak masalah informasi terhadap kelanjutan proses bisnis Bank.

5.2.2. Komite Pengarah Teknologi Informasi (*IT Steering Committee*)

Komite Pengarah Teknologi Informasi bertanggung jawab untuk memberikan rekomendasi kepada direksi paling kurang mengenai hal-hal sebagai berikut:

- a. kebijakan pengamanan informasi sebagai bagian dari Rencana Strategis TI;
- b. efektivitas implementasi kebijakan pengamanan informasi Bank;
- c. efektivitas langkah-langkah mitigasi risiko yang dilakukan untuk meningkatkan pengamanan informasi Bank.

5.2.3 Direksi

Tanggung jawab Direksi untuk pengamanan informasi paling kurang mencakup hal-hal sebagai berikut:

- a. menetapkan kebijakan, sistem dan prosedur pengamanan informasi;
- b. mendukung semua aspek program pengamanan informasi;
- c. menetapkan pembagian tugas dan tanggung jawab untuk pengambilan keputusan terkait manajemen risiko pengamanan informasi;
- d. menetapkan tingkat risiko pengamanan informasi yang dapat diterima oleh Bank;
- e. melakukan evaluasi terhadap hasil penerapan mitigasi risiko pengamanan informasi;
- f. mengkomunikasikan kepada satuan kerja pengguna TI dan penyelenggara TI tentang pentingnya melakukan pengamanan informasi agar Bank dapat mencapai tujuan pengamanan informasi yang diharapkan sesuai ketentuan yang berlaku.

5.2.4. Pejabat Tertinggi Pengamanan Informasi

Sesuai dengan kebijakan dan arahan Direksi, Pejabat Tertinggi Pengamanan Informasi bertanggung jawab atas antara lain:

- a. pengelolaan fungsi pengamanan informasi agar sesuai dengan kebijakan dan ketentuan serta *best practice* yang berlaku;
- b. pemantauan pelaksanaan pengamanan informasi di setiap bagian atau satuan kerja;
- c. mengkomunikasikan program pengamanan informasi termasuk melakukan upaya peningkatan kesadaran akan pengamanan (*security awareness program*);
- d. menetapkan kriteria dan definisi pengukuran risiko pengamanan informasi;
- e. melaksanakan program penilaian risiko pengamanan informasi termasuk menilai kepatuhan seluruh bagian di Bank terhadap kebijakan pengamanan informasi dan merekomendasikan pengendalian yang perlu dilakukan;
- f. memastikan pihak ketiga yang memiliki akses terhadap informasi rahasia milik Bank telah menerapkan pengamanan informasi secara memadai dan konsisten;
- g. membantu koordinasi pengujian BCP;
- h. mengkoordinasikan upaya pengamanan informasi dengan audit intern TI.

5.3. PRINSIP, KEBIJAKAN DAN PROSEDUR PENGAMANAN INFORMASI

5.3.1 Prinsip Pengamanan Informasi

Pengamanan informasi sekurang-kurangnya memperhatikan prinsip-prinsip sebagai berikut:

- a. dilaksanakan untuk meyakini bahwa informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaannya (*availability*) secara

efektif dan efisien dengan memperhatikan kepatuhan (*compliance*) terhadap ketentuan yang berlaku;

- b. memperhatikan aspek sumber daya manusia, proses dan teknologi;
- c. dilakukan berdasarkan hasil penilaian risiko (*risk assessment*) dengan memperhatikan strategi bisnis Bank dan ketentuan yang berlaku;
- d. menerapkan pengamanan informasi secara komprehensif dan berkesinambungan yaitu dengan menetapkan tujuan dan kebijakan pengamanan informasi, mengimplementasikan pengendalian pengamanan informasi, memantau dan mengevaluasi kinerja serta keefektifan kebijakan pengamanan informasi serta melakukan penyempurnaan.

Disamping hal-hal tersebut diatas, Bank perlu mempertimbangkan implementasi standar internasional di bidang pengamanan informasi seperti ISO, IEC, COBIT, IT-IL dan standar nasional seperti SNI, dengan memperhatikan kompleksitas usaha yang meliputi antara lain keragaman dalam jenis transaksi/produk/jasa dan jaringan kantor serta teknologi pendukung yang digunakan.

5.3.2. Kebijakan Pengamanan Informasi

Manajemen Bank harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus dikomunikasikan secara berkala kepada seluruh pegawai Bank dan pihak eksternal yang terkait. Disamping itu dilakukan evaluasi secara berkala dan apabila terdapat perubahan penting. Kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya:

- a. tujuan pengamanan informasi yang sekurang-kurangnya meliputi pengelolaan aset, sumber daya manusia, 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. prinsip dan standar pengamanan informasi, termasuk kepatuhan terhadap ketentuan yang berlaku, pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi (*security awareness program*), rencana kelangsungan bisnis dan sanksi atas pelanggaran;
- e. tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi;
- f. dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

5.3.3. Prosedur Pengamanan Informasi

5.3.3.1. Prosedur Pengelolaan Aset

- a. aset Bank yang terkait dengan informasi harus diidentifikasi, ditentukan pemilik/penanggungjawabnya dan dicatat agar dapat dilindungi secara tepat;
- b. aset yang terkait dengan informasi tersebut dapat berupa data (baik *hardcopy* maupun *softcopy*), perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC) dan sumber daya manusia (termasuk kualifikasi dan ketrampilan);
- c. informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya. Contoh dari klasifikasi tersebut adalah informasi "rahasia" (misalnya data simpanan nasabah, data pribadi nasabah), "internal" (misalnya peraturan tentang gaji pegawai Bank) dan "biasa" (misalnya informasi tentang produk perbankan yang ditawarkan ke masyarakat). Klasifikasi dapat dibuat berdasarkan nilai, sensitivitas, hukum/ketentuan dan tingkat kepentingan bagi Bank.

5.3.3.2. Prosedur Pengelolaan Sumber Daya Manusia

- a. sumber daya manusia baik pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa yang memiliki akses terhadap informasi harus memahami tanggung jawabnya terhadap pengamanan informasi;
- b. peran dan tanggung jawab sumber daya manusia baik pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi;
- c. dalam perjanjian atau kontrak dengan pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa harus tercantum ketentuan-ketentuan mengenai pengamanan Teknologi Informasi 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;
- d. selain perjanjian antara Bank dengan perusahaan penyedia jasa, semua pegawai perusahaan penyedia jasa tersebut yang ditugaskan di Bank harus menandatangani suatu perjanjian menjaga kerahasiaan informasi (*non-disclosure agreement*);
- e. pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab pegawai serta pihak penyedia jasa;
- f. Bank harus menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi;
- g. Bank harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan pengubahan/penutupan hak akses pegawai Bank,

konsultan, pegawai honorer dan pegawai pihak penyedia jasa yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak.

5.3.3.3. Prosedur Pengamanan Fisik dan Lingkungan

- a. fasilitas pemrosesan informasi yang penting (misalnya *mainframe*, *server*, PC, perangkat jaringan aktif) juga harus diberikan pengamanan secara fisik dan lingkungan yang memadai untuk mencegah akses yang tidak terotorisasi, kerusakan serta 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*, PIN, *biometrics*), kelengkapan alat pengamanan di dalam ruangan (misalnya *alarm*, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, *close-circuit TV*) serta pemeliharaan kebersihan ruangan dan peralatan (misalnya dari debu, rokok, makanan/minuman, barang mudah terbakar);
- c. fasilitas pendukung seperti AC, sumber daya listrik, *fire alarm* harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;
- d. aset milik pihak penyedia jasa (seperti *server*, *switching tools*) harus diidentifikasi secara jelas dan diberikan perlindungan yang memadai seperti misalnya dengan menerapkan pengamanan yang cukup, *dual control* atau menempatkan secara terpisah dari aset milik Bank;
- e. harus dilakukan pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan.

5.3.3.4. Prosedur Pengamanan Logic (*Logical Security*)

- a. Bank harus memiliki prosedur formal (tertulis dan telah disetujui oleh manajemen) tentang pengadministrasian *user* yang meliputi pendaftaran, perubahan dan penghapusan *user*, baik untuk *user* internal Bank maupun *user* eksternal Bank (misalnya vendor atau pihak penyedia jasa);
- b. Bank harus menetapkan prosedur pengendalian melalui pemberian *password* awal (*initial password*) kepada *user* dengan memperhatikan antara lain hal-hal sebagai berikut:
 - 1) *password* awal harus diganti saat login pertama kali;
 - 2) *password* awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas berlapis dua;
 - 3) *password* 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 harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan *user-id* dan *password* saat menerima *user-id* dan *password*;
 - 5) *Password* standar (*default password*) yang dimiliki oleh sistem operasi, sistem aplikasi, *database management system*, dan perangkat jaringan harus diganti oleh Bank sebelum diimplementasikan dan sedapat mungkin mengganti user ID standar dari sistem (*default user ID*).
- c. Bank harus mewajibkan *user* untuk:
- 1) menjaga kerahasiaan *password*;
 - 2) menghindari penulisan *password* di kertas dan tempat lain tanpa pengamanan yang memadai;
 - 3) memilih *password* yang berkualitas yaitu:
 - a) panjang *password* yang memadai sehingga tidak mudah ditebak;
 - b) mudah diingat dan terdiri dari sekurang-kurangnya kombinasi 2 tipe karakter (huruf, angka atau karakter khusus);
 - c) tidak didasarkan atas data pribadi user seperti nama, nomor telepon atau tanggal lahir;
 - d) tidak menggunakan kata yang umum dan mudah ditebak oleh perangkat lunak (untuk menghindari *brute force attack*), misalnya kata '*pass*', '*password*', '*adm*', atau kata umum di kamus;
 - 4) mengubah *password* secara berkala;
 - 5) menghindari penggunaan *password* yang sama secara berulang.
- d. Bank harus menonaktifkan hak akses bila *user id* tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan *password* (*failed login attempt*) dan menonaktifkan *password* setelah mencapai jumlah maksimal kegagalan *password*;
- e. Bank harus melakukan pemeriksaan/*review* berkala terhadap hak akses *user* untuk memastikan bahwa hak akses yang diberikan sesuai dengan wewenang yang diberikan.
- f. Sistem operasi, sistem aplikasi, *database*, *utility* dan perangkat lainnya yang dimiliki oleh Bank sedapat mungkin membantu pelaksanaan pengamanan *password*, sebagai contoh:
- 1) memaksa *user* untuk mengubah *password*nya setelah jangka waktu tertentu dan menolak bila *user* memasukkan *password* yang sama dengan yang digunakan sebelumnya saat mengganti *password*;
 - 2) menyimpan *password* secara aman (ter-enkripsi);
 - 3) memutuskan hubungan atau akses *user* jika tidak terdapat respon selama jangka waktu tertentu (*session time-out*);

- 4) menonaktifkan atau menghapus hak akses *user* jika *user* tidak melakukan *log-on* melebihi jangka waktu tertentu (*expiration interval*), misalnya karena cuti, pindah bagian.
- g. Bank harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai dalam penggunaan perangkat *mobile computing* dan media penyimpan data seperti *notebook*, *hand phone*, *personal digital assistance*, *flash disk*, *external hard disk*, termasuk bila menggunakan *wireless access* atau *wireless network*;
- h. Bank harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai terhadap titik akses (*access point*) ke dalam jaringan komputer dan/atau sarana pemrosesan informasi yang dapat dimanfaatkan oleh pihak yang tidak berwenang;
- i. Bank yang menggunakan *file sharing* harus menetapkan pembatasan akses sekurang-kurangnya melalui penggunaan *password* dan pengaturan pihak yang berwenang melakukan akses;
- j. Bank perlu memperhatikan proses *security hardening* terhadap perangkat keras dan perangkat lunak, seperti : *setting parameter*, *patch*.

5.3.3.5. Prosedur Pengamanan Operasional Teknologi Informasi

Hal-hal yang harus diperhatikan dalam pengamanan operasional TI antara lain:

- a. informasi dan perangkat lunak harus dibuatkan *backup* dan *prosedur recovery* yang teruji sesuai dengan tingkat kepentingannya;
- b. Bank perlu mengantisipasi dan menerapkan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, *database* dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti *virus*, *trojan horse*, *worms*, *spyware*, *Denial-Of-Service (DOS)*, *war driving*, , *spoofing* dan *logic bomb*;
- c. Bank harus memiliki kebijakan dan prosedur pengkinian anti-virus dan *patch* dan memastikan pelaksanaannya;
- d. Bank harus membuat prosedur yang mencakup identifikasi *patch* yang ada, melakukan pengujian, dan menginstalasinya jika memang dibutuhkan;
- e. Bank juga harus memelihara catatan dari versi perangkat lunak yang digunakan dan memantau secara rutin informasi tentang pengkinian (*enhancement*) produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan;
- f. Bank harus menetapkan penggunaan enkripsi dengan menggunakan teknik kriptografi tertentu dalam mengamankan proses transmisi informasi yang sensitif, khususnya yang melalui jaringan di luar jaringan komunikasi Bank, sesuai dengan perkembangan teknologi terkini. Penggunaan teknik kriptografi tersebut antara lain

- ditujukan untuk menjaga dan memastikan kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authenticity*), dan *non-repudiation*. Teknik yang dapat dipertimbangkan antara lain penggunaan enkripsi, *hash function*, dan *digital signatures* (menggunakan *Public Key Infrastructure*);
- g. Bank harus menerapkan metode identifikasi dan otentikasi (*authentication*) sesuai tingkat pentingnya aplikasi misalnya penggunaan *one-factor authentication* untuk aplikasi “biasa” serta *penggunaan two-factor authentication* untuk aplikasi bersifat “kritis”;
 - h. Contoh metode identifikasi dan otentikasi antara lain *log on id* dan *password*, *token device* atau *biometrics* (misalnya *fingerprint*, *retina scan*, *face/iris/hand/palm analysis*, *signature recognition*, *voice recognition*);
 - i. Bank harus menyediakan dan melakukan kaji ulang atas jejak audit/log baik di tingkat jaringan, sistem maupun aplikasi serta menetapkan jenis *log* (misalnya *administrator log*, *user log*, *system log*), informasi yang harus dimasukkan ke dalam *log*, jangka waktu penyimpanan atau kapasitas *log* dengan memperhatikan ketentuan yang berlaku untuk keperluan penelusuran masalah.

5.3.3.6. Prosedur Penanganan Insiden dalam Pengamanan Informasi

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

- a. insiden yang terjadi harus dapat diidentifikasi, dilaporkan, ditindaklanjuti, didokumentasikan dan dievaluasi untuk memastikan dilakukannya penanganan yang tepat dan untuk mencegah terulangnya insiden;
- b. Bank harus menetapkan prosedur penanganan insiden yang mengatur antara lain:
 - 1) Siapa yang harus melaporkan insiden;
 - 2) Jenis insiden yang harus dilaporkan;
 - 3) Alur pelaporan insiden (*point of contact*);
 - 4) Siapa yang bertanggung jawab untuk menindaklanjuti insiden;
 - 5) Analisis atas insiden untuk mencegah terulangnya insiden;
 - 6) Pendokumentasian bukti terkait insiden dan tindak lanjutnya.
- c. Bank perlu mempertimbangkan pembentukan tim khusus yang menangani insiden pengamanan (CSIRT – *Computer Security Incident Response Team* atau CERT – *Computer Emergency Response Team*) sesuai dengan skala usaha dan kompleksitas TI Bank;
- d. Pegawai Bank, pegawai honorer dan pegawai pihak penyedia jasa diminta untuk melaporkan setiap kali menemukan indikasi atau potensi kelemahan pada sistem dan aplikasi sesuai kebijakan dan prosedur pelaporan insiden pengamanan. Kelemahan yang perlu dilaporkan misalnya adanya virus dari *e-mail* yang masuk.

5.3.3.7. Prosedur lainnya

Selain ruang lingkup diatas, pengamanan informasi perlu diterapkan dalam aspek lain seperti pengembangan dan pengadaan sistem, jaringan komunikasi data, BCP dan DRP dan kegiatan penggunaan pihak penyedia jasa dalam penyelenggaraan TI.

5.4 PROSES MANAJEMEN RISIKO

5.4.1. Penilaian Risiko

Mengingat pentingnya TI dalam mendukung tercapainya rencana strategis bisnis Bank, maka Bank harus mengelola seluruh sumber daya TI sebagai "aset" Bank. Sumber daya TI meliputi antara lain aplikasi, informasi, infrastruktur dan sumber daya manusia. Untuk itu Bank harus melakukan evaluasi atas segala hal yang mengancam sumber daya TI melalui proses identifikasi, pengukuran dan pemantauan risiko potensial baik kecenderungan atau probabilitas terjadinya maupun besarnya dampak.

Terdapat berbagai pendekatan yang dapat dilakukan Bank dalam proses identifikasi seperti pendekatan proses, aset, produk, dan kejadian. Pada pendekatan berdasarkan aset, identifikasi risiko pengamanan informasi dilakukan dengan melakukan klasifikasi terhadap "aset" terkait teknologi informasi berdasarkan risiko. Selanjutnya Bank melakukan pengukuran kecenderungan atau probabilitas terjadinya risiko atas setiap aset dan besarnya dampak kerugian yang akan dialami untuk dapat mengetahui besarnya risiko potensial yang harus dihadapi atau Nilai Risiko Dasar (NRD). Contoh penilaian risiko pengamanan informasi yang menggunakan pendekatan aset dapat dilihat di Lampiran 1.1. Penilaian ini dilakukan oleh setiap satuan kerja yang memiliki sumber daya TI dan atau dapat dikoordinasikan oleh satuan kerja yang membidangi TI atau manajemen risiko. Dalam menentukan aset yang kritikal maupun mengukur risiko, setiap satuan kerja harus dapat menentukan kemungkinan adanya ancaman (*threats*), serangan (*attacks*) dan kerawanan (*vulnerability*) dari setiap sumber daya TI yang digunakan masing-masing satuan kerja serta kemungkinan dampaknya pada integritas (*integrity*), kerahasiaan (*confidentiality*) dan ketersediaan (*availability*) dari data/informasi yang dimiliki. Proses ini harus dilakukan Bank karena identifikasi dan pengukuran risiko dapat menunjukkan potensial kegagalan atau kelemahan proses pengamanan informasi yang dapat berpengaruh pada kesuksesan bisnis Bank sehingga Bank dapat melakukan penanganan yang tepat terhadap setiap risiko potensial.

5.4.2. Pengendalian Dan Mitigasi Risiko

Berdasarkan hasil identifikasi dan pengukuran risiko, Bank harus menetapkan bentuk penanganan risiko yang akan diterapkan untuk meminimalisasi risiko yang dihadapi Bank. Dari bentuk-bentuk penanganan risiko (*accept, control/mitigate, avoid,*

transfer), pengendalian dan atau mitigasi risiko memegang peranan penting karena tanpa sistem informasi yang handal dan aktivitas pengendalian TI yang efektif, Bank tidak mampu menghasilkan laporan keuangan yang akurat, terkini, utuh dan lengkap. Secara umum bentuk pengendalian antara lain:

- a. kebijakan, ketentuan dan prosedur yang ada di Bank;
- b. sistem pengendalian risiko yang dilakukan dengan menggunakan teknologi sehingga secara otomatis dapat memitigasi risiko yang ada seperti *audit log*, *on line approval*, *parameter value* di sistem yang digunakan;
- c. *training* dan *security awareness program*.

Tinjauan atas pengendalian dilakukan dua kali yaitu pertama pada proses penilaian risiko (*risk assessment*) dimana Bank mengidentifikasi pengendalian yang telah ada sebelumnya, dan kedua setelah mendapatkan Nilai Risiko Akhir (*residual risk*). Dengan membandingkan Nilai Risiko Dasar (NRD) dengan Nilai Risiko Akhir (NRA), Bank dapat menganalisis kelemahan dari bentuk pengendalian yang telah diterapkan dan bentuk pengendalian pengamanan yang dapat direkomendasikan untuk diterapkan kemudian. Bentuk pengendalian dapat beragam dan tidak terbatas pada pengendalian umum (*general controls*) seperti pengendalian yang harus ada di operasional *Data Center* maupun yang berupa pengendalian aplikasi (*application controls*) seperti rekonsiliasi dalam *balancing control activities*. Dengan demikian atas seluruh aset Bank baik pada level Bank, satuan kerja maupun masing-masing petugas/pengguna TI dapat terhindar dari setiap risiko potensial.

5.5. PENGENDALIAN INTERN DAN AUDIT INTERN

Auditor Intern TI harus melaksanakan program audit untuk memastikan bahwa pengendalian pengamanan informasi telah diterapkan, memadai dan berjalan secara efektif sesuai dengan kebijakan dan prosedur pengamanan informasi yang berlaku. Pengendalian intern harus diterapkan dalam pengamanan informasi karena pengamanan informasi adalah sebuah proses dinamis yang harus dilakukan secara berkesinambungan. Evaluasi dan penyempurnaan terhadap kebijakan, prosedur dan program pengamanan informasi harus selalu dilakukan 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 *trend* ancaman atau kelemahan kontrol pengamanan. Secara lebih spesifik kegiatan ini meliputi kaji ulang terhadap *log* aktivitas, investigasi anomali operasional dan secara rutin mengevaluasi level akses terhadap sistem dan aplikasi TI;
- c. tindak lanjut penanganan serangan atau insiden pengamanan informasi terhadap Bank;
- d. efektivitas penerapan kebijakan, prosedur dan pengendalian pengamanan informasi;

- e. kegiatan pencegahan terjadinya risiko potensial atas kemungkinan ancaman terhadap keamanan informasi/sistem informasi seperti misalnya:
- 1) pembuatan proses yang memantau ancaman terhadap *hardware/software*, instalasi *security patches*;
 - 2) pengecekan pengkinian/*updating* anti virus;
 - 3) pengawasan terhadap jasa-jasa pihak ketiga/*vendor*.

Pemantauan pengamanan informasi meliputi aspek teknis dan non-teknis. Aspek non-teknis meliputi perubahan organisasi, perubahan proses bisnis, lokasi baru, perubahan tingkat sensitivitas informasi atau penerbitan produk/jasa baru. Aspek teknis meliputi sistem baru, penyedia jasa yang baru, dan perluasan/penambahan akses terhadap informasi. Pemantauan tersebut dapat dilakukan oleh *information security officer* atau apabila Bank tidak memilikinya maka dilakukan oleh pegawai Bank yang berfungsi mengelola program pengamanan informasi. Namun demikian setiap karyawan dan manajemen harus tetap waspada terhadap ancaman terhadap keamanan informasi/sistem informasi.

BAB VI

BUSINESS CONTINUITY PLAN

6.1. PENDAHULUAN

Kegiatan perbankan tidak dapat terhindar dari adanya gangguan/kerusakan yang disebabkan oleh alam maupun manusia misalnya terjadinya gempa bumi, bom, kebakaran, banjir, *power failure*, kesalahan teknis, kelalaian manusia, demo buruh, huru-hara dan sebagainya. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi suatu Bank, tetapi juga berdampak pada kegiatan operasional bisnis Bank terutama pelayanan kepada nasabah. Bila tidak ditangani secara khusus, selain Bank akan menghadapi risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan nasabah kepada Bank.

Untuk meminimalisasi risiko tersebut, Bank diharapkan memiliki *Business Continuity Management* (BCM) yaitu proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional Bank tetap dapat berfungsi walaupun terdapat gangguan/bencana guna melindungi kepentingan para *stakeholder*. BCM merupakan bagian yang terintegrasi dengan kebijakan manajemen risiko Bank secara keseluruhan. BCM yang efektif perlu didukung dengan hal-hal sebagai berikut:

- a. adanya pengawasan aktif manajemen;
- b. melalui *Business Impact Analysis* dan *Risk Assessment*;
- c. penyusunan *Business Continuity Plan* yang memadai;
- d. dilakukannya pengujian terhadap BCP; dan
- e. dilakukan pemeriksaan oleh Auditor Intern.

Business Continuity Plan (BCP) merupakan suatu dokumen tertulis yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan/bencana dan proses pemulihan agar kegiatan operasional Bank dan pelayanan kepada nasabah tetap dapat berjalan. Rencana tindak tertulis tersebut melibatkan seluruh sumber daya Teknologi Informasi (TI) termasuk sumber daya manusia yang mendukung fungsi bisnis dan kegiatan operasional yang kritical bagi Bank.

Komponen prosedur BCP yang harus dimiliki Bank paling kurang meliputi *Disaster Recovery Plan* (DRP) dan *Contingency Plan* (CP). *Disaster Recovery Plan* (DRP) lebih menekankan pada aspek teknologi dengan fokus pada *data recovery/restoration plan* dan berfungsinya sistem aplikasi dan infrastruktur TI yang kritical. Sedangkan *Contingency Plan* (CP) menekankan pada rencana tindak untuk menjaga kelangsungan bisnisnya apabila terjadi gangguan atau bencana termasuk tindakan antisipatif menghadapi kondisi terburuk misalnya bila TI yang digunakan

sama sekali tidak dapat dipulihkan untuk waktu yang cukup lama. *Contingency Plan (CP)* harus meliputi pula rencana untuk memastikan kelangsungan seluruh pelayanan Bank termasuk yang dilaksanakan melalui *electronic banking*.

6.2. PENGAWASAN AKTIF MANAJEMEN

Efektifitas dari BCP akan sangat bergantung pada komitmen manajemen untuk menyediakan sumber daya yang diperlukan dalam rangka mengidentifikasi, menyusun dan melakukan pengujian terhadap BCP.

6.2.1. Peran dan Tanggung Jawab Direksi

- a. menetapkan kebijakan, strategi dan prosedur BCP;
- b. menetapkan BCP yang dikinikan secara berkala;
- c. memastikan adanya suatu organisasi atau tim kerja yang bertanggungjawab atas BCP, yang terdiri dari personil yang kompeten dan terlatih;
- d. meyakini bahwa BCP disosialisasikan kepada seluruh fungsi bisnis dan personil;
- e. menelaah hasil kaji ulang atas pengujian BCP yang dilakukan secara reguler;
- f. mengevaluasi hasil pemeriksaan audit intern atas kecukupan BCP.

6.2.2. Peran dan Tanggung Jawab Tim Kerja BCP

Agar BCP dapat berjalan dengan baik pada saat diperlukan, maka bank perlu membentuk suatu organisasi atau tim kerja untuk mengkoordinasi pelaksanaan BCP, yang terdiri dari:

- a. koordinator;
- b. anggota tim yang memiliki tanggung jawab terhadap:
 - 1) satuan kerja bisnis;
 - 2) satuan kerja TI antara lain *offsite storage*, aplikasi, perangkat keras dan perangkat lunak, *network*, *security*, *communication*, *data preparation and records*;
 - 3) unit pendukung lainnya seperti Satuan Kerja Logistik, Pengamanan dan Umum, Hubungan Masyarakat dan Legal, Sumber Daya Manusia.

Adapun peran tim kerja penanggung jawab BCP di atas sekurang-kurangnya meliputi:

- a. bertanggung jawab penuh terhadap efektivitas penyelenggaraan BCP, termasuk memastikan bahwa program *awareness* atas BCP diterapkan;
- b. memutuskan kondisi *disaster* dan pemulihannya;
- c. menentukan skenario pemulihan yang akan digunakan bila terjadi gangguan atau bencana berdasarkan prioritasitas atas aktivitas, fungsi dan jasa yang dianggap kritis;
- d. *me-review* laporan mengenai setiap tahapan dalam pengujian dan pelaksanaan BCP;
- e. melaksanakan komunikasi kepada pihak intern dan ekstern Bank bila terjadi suatu gangguan operasional yang bersifat *major*.

6.3. PRINSIP-PRINSIP PENYUSUNAN BCP

Dalam penyusunan kebijakan, strategi dan prosedur yang akan diterapkan untuk menangani keadaan *disaster*, Bank harus memastikan diterapkannya prinsip-prinsip sebagai berikut:

- a. penyusunan BCP hendaknya melibatkan seluruh satuan kerja dan fungsi bisnis, bukan hanya satuan kerja TI;
- b. BCP disusun berdasarkan *Business Impact Analysis* dan *Risk Assessment* yang memadai;
- c. BCP bersifat fleksibel untuk dapat merespon berbagai skenario ancaman dan gangguan serta bencana yang sifatnya tidak terduga baik bersumber dari kondisi internal maupun eksternal;
- d. BCP bersifat spesifik, terdapat kondisi-kondisi tertentu dan tindakan yang dibutuhkan segera dilakukan untuk kondisi tersebut;
- e. dilakukan pengujian dan pengkinian secara berkala;
- f. BCP dan hasil pengujian BCP harus dikaji ulang oleh audit intern secara berkala.

6.4. BUSINESS IMPACT ANALYSIS

Efektifitas dari suatu BCP akan sangat bergantung pada kemampuan manajemen untuk secara tepat mengidentifikasi kritis tidaknya berbagai proses kerja atau aktivitas yang ada di Bank sebelum BCP disusun atau dikaji ulang. Dengan demikian *Business Impact Analysis* (BIA) merupakan dasar dari penyusunan keseluruhan BCP. Hal-hal yang harus dianalisis dalam BIA meliputi:

- a. tingkat kepentingan (*criticality*) masing-masing proses bisnis dan ketergantungan antar proses bisnis serta prioritas yang diperlukan;
- b. tingkat ketergantungan terhadap pihak penyedia jasa baik TI maupun non TI;
- c. tingkat *Maximum Tolerable Outage/Recovery Time Objective* (berapa lama bank dapat bekerja tanpa sistem atau fasilitas yang mengalami gangguan dan atau berapa cepat sistem atau fasilitas tersebut harus berfungsi kembali);
- d. tingkat *Minimum Resources Requirement* (personil, data dan kelengkapan sistem serta fasilitas yang diperlukan secara minimal agar bisnis bisa pulih dan berjalan);
- e. dampak potensial dari kejadian yang bersifat tidak spesifik dan tidak dapat dikontrol terhadap proses bisnis dan pelayanan kepada nasabah;
- f. dampak *disaster* terhadap seluruh departemen dan fungsi bisnis, bukan hanya terhadap *data processing*;
- g. estimasi *downtime* maksimum yang dapat ditoleransi dan tingkat toleransi atas kehilangan data dan terhentinya proses bisnis serta dampak *downtime* terhadap kerugian finansial;
- h. jalur komunikasi yang dibutuhkan untuk berjalannya pemulihan;

- i. kemampuan dan pengetahuan petugas mengenai *Contingency Plan* dan ketersediaan petugas pengganti di tempat pemulihan;
- j. dampak hukum dan pemenuhan ketentuan yang terkait, seperti ketentuan mengenai kerahasiaan data nasabah.

Dalam melakukan BIA di atas, baik satuan kerja TI maupun masing-masing unit bisnis perlu memperhatikan bahwa BCP yang akan disusun bukan hanya untuk *total disaster* namun untuk berbagai situasi bencana dan gangguan mulai dari yang *minor*, *major* sampai dengan *catastrophic*.

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

6.5. PENILAIAN RISIKO

Penilaian risiko (*risk assessment*) yang terdiri dari identifikasi dan pengukuran risiko merupakan tahap kedua yang harus dilalui dalam penyusunan suatu BCP. Proses ini diperlukan untuk dapat mengetahui tingkat kemungkinan terjadi gangguan pada kegiatan bank yang penting (*critical*) serta dampaknya bagi kelangsungan usaha bank. *Risk assessment* sekurang-kurangnya mencakup hal-hal sebagai berikut:

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

6.6. PROSES PENYUSUNAN BUSINESS CONTINUITY PLAN

Penyusunan BCP dilakukan setelah proses BIA dan *Risk Assessment*. Adapun tujuan dan sasaran dari penyusunan BCP antara lain:

- a. mengamankan aset penting bank;
- b. meminimalisasi risiko akibat *disaster* misalnya membatasi kerugian finansial, risiko hukum dan reputasi;
- c. meyakini ketersediaan layanan yang berkesinambungan kepada nasabah; dan
- d. mempersiapkan alternatif lain agar fungsi bisnis yang kritikal tetap dapat berjalan untuk menjaga kelangsungan operasi bank.

BCP terdiri dari kebijakan, strategi, skenario dan prosedur yang diperlukan untuk dapat memastikan kelangsungan proses bisnis pada saat terjadinya gangguan atau bencana. BCP 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 BIA, analisis risiko, sumber daya yang dimiliki serta kapasitas dan tingkat teknologi Bank. Contoh strategi yang dapat dipilih antara lain, penggunaan jasa pihak lain (*outsourcing*), *Disaster Recovery Center (hot site, warm site atau cold site)* dan atau *Business Recovery Center*. Setiap strategi yang dipilih hendaknya disertai analisis/alasan yang melatarbelakangi dan harus didukung dengan sistem dan prosedur yang sesuai.

6.6.1. Jenis Prosedur BCP

Adapun jenis-jenis prosedur dalam BCP antara lain mencakup:

- a. prosedur tanggap darurat (*emergency response - immediate steps*) untuk mengendalikan krisis pada saat terjadi gangguan/bencana, membatasi dampak kerugian, serta menentukan perlu tidaknya mendeklarasikan keadaan *disaster*;
- b. prosedur pemulihan sistem yang memungkinkan kegiatan operasional Bank dapat kembali ke kondisi normal;
- c. prosedur pemulihan bisnis (*business recovery*) yang menjabarkan tugas dan tanggung jawab di masing-masing proses bisnis agar dapat segera memulihkan kegiatan operasional Bank. Termasuk dalam hal ini *contingency plan* untuk pelayanan nasabah secara manual apabila dibutuhkan;
- d. prosedur sinkronisasi data 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.

6.6.2. Komponen Prosedur BCP

Setiap prosedur BCP di atas hendaknya sekurang-kurangnya mencakup komponen sebagai berikut:

a. Personil:

Apabila diperlukan, dalam organisasi tim kerja BCP dapat dibentuk sub-sub tim untuk koordinasi, pelaksanaan prosedur tanggap darurat, pelaksanaan pemulihan sistem, pelaksanaan pemulihan proses bisnis dan evaluasi atau umpan balik. BCP harus secara jelas mengemukakan komposisi, wewenang dan tanggung jawab setiap tim kerja tim kerja BCP dan memiliki alur komunikasi yang terintegrasi.

b. 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 DRC dan dokumentasi sistem dan *data backup*.

c. *Disaster Recovery Center (DRC)*:

Bank harus memastikan ketersediaan DRC sebagai *backup DC* yang dapat dioperasikan apabila DC tidak dapat beroperasi atau dalam kondisi *disaster*. Sesuai

dengan alternatif strategi yang dipilih Bank, DRC dapat dikelola sendiri maupun oleh pihak penyedia jasa. Bank harus memperhatikan hal-hal sebagai berikut:

- 1) DRC hendaknya ditempatkan pada lokasi yang terpisah dari lokasi DC, dengan memperhatikan faktor geografi:
 - a) jangkauan geografi atas suatu gangguan/bencana dan dampaknya terhadap kota atau wilayah tempat lokasi DRC berada;
 - b) analisis risiko yang berkaitan dengan lokasi DRC (apakah wilayah gempa atau petir) dan terhubung dengan infrastruktur komunikasi dan listrik yang berbeda dengan DC, serta fasilitas lain yang diperlukan untuk tetap berjalannya suatu sistem;
 - 2) kondisi rentannya lokasi yang dipilih dengan kemungkinan huru-hara dan kerusuhan;
 - 3) DRC harus memiliki pasokan listrik dan sarana telekomunikasi yang dapat menjamin beroperasinya DRC;
 - 4) sistem di DRC harus kompatibel dengan sistem yang digunakan pada DC dan harus disesuaikan jika terjadi perubahan pada DC;
 - 5) merupakan *restricted area*; dan
 - 6) memperhitungkan waktu tempuh untuk terjaminnya proses *recovery*.
- d. *Backup* Dokumentasi, Sistem dan Data
- Bank harus meyakini ketersediaan *backup* yang efektif dari informasi bisnis yang penting, perangkat lunak dan dokumentasi terkait sistem dan *user* untuk setiap proses fungsi bisnis yang penting (*critical*). Hal-hal yang harus diperhatikan dalam dokumentasi, sistem dan *data backup* antara lain:
- 1) *backup* dimaksud harus disimpan di lokasi lain dari DC (*off site*). Setiap perubahan dan modifikasi harus didokumentasikan dan salinannya juga harus diperbaharui;
 - 2) media *backup* harus disimpan di lingkungan yang aman di lokasi *off site* dengan standar sistem pengamanan yang memadai;
 - 3) *full system backup* harus dilakukan secara periodik. Jika terjadi perubahan sistem yang mendasar maka *full system backup* harus dilakukan sesegera mungkin;
 - 4) seluruh media *backup* menggunakan standar *labeling*/penamaan untuk dapat mengidentifikasi penggunaan, tanggal dan jadual retensi;
 - 5) media *backup* harus diuji secara regular untuk meyakini bahwa dapat digunakan pada saat diperlukan (keadaan *emergency*);
 - 6) Bank harus memiliki prosedur untuk *disposal* media *backup*.
- e. *Business Recovery Center (BRC)/Crisis Center/Business Resumption Center*
- BCP harus memiliki skenario mengenai lokasi kegiatan dari masing-masing fungsi bisnis untuk berbagai tingkat *disaster*. Untuk tingkat bencana *total disaster* atau *catastrophic*, Bank sebaiknya menyiapkan lokasi alternatif agar tetap dapat menjalankan kegiatan fungsi bisnis.

f. Fasilitas Komunikasi

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

6.7. PENGUJIAN BCP

Pengujian BCP diperlukan untuk meyakini bahwa BCP dapat dioperasikan dengan baik pada saat terjadi gangguan/bencana. Uji coba dilakukan atas BCP dan DRP sekurang-kurangnya 1 (satu) tahun sekali untuk seluruh sistem/aplikasi kritikal (sesuai hasil *Business Impact Analysis*) dan mewakili seluruh infrastruktur yang kritikal serta melibatkan *end user (end to end)*.

Apabila Bank menggunakan pihak penyedia jasa dalam kegiatan operasionalnya maka pengujian yang dilakukan juga perlu melibatkan pihak eksternal tersebut. Dalam hal Bank melakukan perubahan yang sangat mendasar terhadap sistem, aplikasi atau infrastruktur teknologi informasinya (misalnya perubahan pada *core banking system*), maka harus dilakukan pengujian DRP selambat-lambatnya 6 bulan setelah perubahan sistem dimaksud diimplementasikan.

6.7.1. Ruang Lingkup Pengujian BCP

Manajemen harus secara jelas menentukan fungsi, sistem dan proses apa saja yang akan diuji. Hal-hal yang perlu dilakukan pengujian antara lain meliputi efektifitas dari:

- a. prosedur evakuasi personil dan jalur komunikasi yang ditetapkan (*call tree*);
- b. prosedur penetapan kondisi *disaster*;
- c. fasilitas DRC dan BRC yang disediakan oleh pihak lain baik yang hanya untuk Bank sendiri maupun yang digunakan bersama dengan Bank-Bank lain;
- d. prosedur pemulihan atas data penting;
- e. pengembalian kegiatan operasional Bank dan *Data Center* ke lokasi unit bisnis dan pusat data semula.

Pengujian yang dilakukan harus didokumentasikan secara tertib dan dievaluasi untuk meyakini efektifitas dan keberhasilan pengujian. Jika dalam pengujian didapati kelemahan atas BCP, maka BCP perlu disempurnakan.

6.7.2. Test Plan (Skenario Pengujian)

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 BCP.

Dalam hal ini Bank perlu memvalidasi asumsi yang digunakan dalam skenario pengujian/*test plan*, antara lain mengenai:

- a. tingkat kritikal proses fungsi bisnis atau sistem yang diuji;
- b. volume transaksi;
- c. ketergantungan antar proses bisnis;
- d. strategi BCP yang dipilih Bank;
- e. ketersediaan dan kecukupan sumber daya yang diperlukan agar sesuai dengan *service level* yang ditetapkan, seperti waktu yang diperlukan untuk mempersiapkan fasilitas yang ada, mempersiapkan *file backup* atau mempersiapkan dokumen.

6.6.3. Analisis dan Laporan Hasil Pengujian

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 BCP dan hasil pengujian serta usulan perubahannya;
- e. rekomendasi untuk pengujian selanjutnya.

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

6.7. PEMELIHARAAN BCP DAN AUDIT INTERN

6.7.1. Pemeliharaan BCP

Bank harus memastikan bahwa BCP dapat digunakan setiap saat antara lain dengan menyimpan salinan dokumen BCP di lokasi alternatif (*alternate site*), meningkatkan pemahaman semua pihak di Bank maupun di penyedia jasa atas pentingnya BCP dan berpartisipasi aktif dalam pelaksanaan BCP. Setiap personil inti di Tim Kerja BCP harus memiliki ringkasan prosedur tanggap darurat BCP serta daftar *contact person* terkini yang harus dihubungi pada saat terjadi gangguan/bencana (*call tree*).

Di samping itu setiap satuan kerja secara berkala harus melakukan *self assessment* kesesuaian *Business Impact Analysis* dengan perubahan yang terjadi dalam kegiatan operasional baik yang diselenggarakan sendiri maupun oleh pihak penyedia jasa.

Bank harus melakukan pengkinian BCP untuk meyakinkan kesesuaiannya dengan kondisi eksternal maupun internal. Dalam melakukan pengkinian, hal-hal yang perlu diperhatikan antara lain perubahan yang ada dalam proses bisnis, struktur organisasi, sistem, *software*, *operating system*, *hardware*, personil/*key staff*, fasilitas, *counterparties* dan *service providers*. Perubahan tersebut harus dianalisa pengaruhnya

terhadap BCP yang ada saat ini dan menentukan perbaikan yang dibutuhkan untuk mengakomodasi perubahan tersebut dalam BCP terbaru. Selanjutnya BCP hasil revisi tersebut harus didokumentasikan dan didistribusikan ke seluruh organisasi.

6.7.2. Audit Intern

Auditor Intern harus melakukan pemeriksaan terhadap:

- a. kesesuaian BCP dengan kebijakan manajemen risiko Bank;
- b. BCP mencakup kegiatan kritikal berdasarkan *Business Impact Analysis*;
- c. kecukupan BCP untuk mengendalikan dan memitigasi risiko yang telah ditetapkan dalam *risk assessment*;
- d. kecukupan prosedur pengujian BCP;
- e. efektifitas pelaksanaan pengujian BCP;
- f. program pelatihan dan sosialisasi BCP;
- g. keterkinian BCP sesuai perkembangan kegiatan operasional Bank dan hasil pengujian terakhir.

Auditor intern harus mengkomunikasikan hasil pemeriksaan dan memberikan rekomendasi kepada direksi. Direksi hendaknya melakukan kaji ulang atas laporan hasil audit tersebut.

BAB VII

END USER COMPUTING

7.1. PENDAHULUAN

End User Computing (EUC) adalah sistem aplikasi komputer yang menjalankan operasi bisnis Bank dimana kendali terhadap pengembangan sistem aplikasi serta pengelolaannya dilakukan oleh satuan kerja pengguna akhir (*end user*) atau unit bisnis Bank dan bukan oleh satuan kerja TI.

Beberapa alasan yang melatarbelakangi penggunaan EUC pada suatu Bank antara lain:

- a. adanya proyek pengembangan sistem aplikasi yang tertunda pelaksanaannya (*backlog project*) oleh satuan kerja TI, sehingga EUC memungkinkan pengguna akhir untuk mengembangkan, memelihara, dan mengoperasikan TI sendiri;
- b. adanya kebutuhan spesifik dari pengguna, dengan jumlah pengguna yang sedikit dan volume yang rendah, sehingga kurang efisien jika melalui prosedur pengembangan sistem aplikasi secara umum oleh satuan kerja TI.

7.2. PERAN DAN TANGGUNG JAWAB MANAJEMEN

Dalam kaitannya dengan EUC, manajemen Bank wajib memastikan bahwa:

- a. risiko-risiko yang dapat timbul terkait dengan EUC telah dikelola dengan memadai;
- b. EUC dapat meningkatkan kinerja satuan kerja pengguna. Sistem aplikasi EUC dapat digunakan untuk memenuhi kebutuhan dalam menganalisis data, membuat laporan, dan melakukan *query* yang memungkinkan proses pengambilan keputusan berlangsung lebih efektif dan efisien;
- c. EUC hanya digunakan untuk memenuhi kebutuhan sistem aplikasi yang tidak kompleks, dapat memenuhi kebutuhan yang selalu berubah, atau untuk memberi respon yang cepat terhadap kebutuhan yang mendesak atau sementara/tidak rutin;
- d. EUC dapat mengurangi penundaan pembuatan (*backlog*) sistem aplikasi;
- e. keterlambatan pemenuhan permintaan modifikasi atau pengembangan sistem aplikasi baru akan berkurang karena EUC mengurangi beban pada pengembangan sistem teknologi informasi oleh Satuan Kerja TI.

7.3. KEBIJAKAN DAN PROSEDUR EUC

Hal-hal yang perlu diatur dalam kebijakan dan prosedur bank mengenai EUC mencakup antara lain:

- a. kebijakan dan prosedur harus tertulis, disetujui oleh Direksi/pejabat yang berwenang, dikaji ulang dan dikinikan secara periodik, serta disosialisasikan kepada seluruh pengguna akhir;
- b. pencantuman secara jelas wewenang dan tanggung jawab manajemen, unit bisnis yang terkait, satuan kerja TI, serta satuan kerja audit intern;
- c. adanya analisis kebutuhan pengembangan sistem aplikasi EUC dan prosedur persetujuannya;
- d. pengembangan sistem aplikasi EUC harus memenuhi standar dan kriteria pengamanan yang ditetapkan oleh satuan kerja TI;
- e. sistem aplikasi yang dimungkinkan untuk dikembangkan secara EUC adalah sistem aplikasi yang memiliki tingkat kompleksitas dan risiko “*low*” hingga “*moderate*” dan harus melalui persetujuan pihak manajemen;
- f. adanya tahap-tahap pengembangan sistem aplikasi EUC, mulai dari pengadaan sampai dengan implementasi;
- g. adanya prosedur perubahan terhadap sistem aplikasi EUC;
- h. memenuhi aspek-aspek pengamanan (fisik dan logik), pengendalian sistem aplikasi EUC (pengendalian atas *input*, proses, dan *output*), pengendalian operasional termasuk pencegahan virus;
- i. tersedianya daftar terkini sistem aplikasi EUC yang ada;
- j. melakukan penyimpanan dan *backup* data/file;
- k. tersedianya dokumentasi yang memadai, mencakup antara lain *user manual* dan *system manual*. Setiap perubahan terhadap sistem aplikasi EUC harus disertai dengan pengkinian dokumentasi tersebut;
- l. jika sistem aplikasi dibuat oleh vendor, satuan kerja pengguna akhir harus melakukan koordinasi dengan satuan kerja TI. Di samping itu manajemen harus memastikan kecukupan pelatihan dan manual yang disusun sebagai bagian dari kontrak antara Bank dan vendor;
- m. apabila aplikasi yang dikembangkan oleh vendor tersebut menyebabkan Bank memiliki ketergantungan yang berkesinambungan terhadap jasa pihak pengembang tersebut maka pemilihan vendor melalui proses yang mengacu pada pedoman tentang Penggunaan Pihak Penyedia Jasa Teknologi Informasi serta kebijakan dan prosedur intern Bank;
- n. kebijakan dan prosedur pengembangan EUC tidak boleh bertentangan dengan kebijakan yang ada khususnya kebijakan pengembangan sistem (SDLC) serta kebijakan pengamanan informasi.

7.4. MANAJEMEN RISIKO EUC

7.4.1. Identifikasi dan Pengukuran Risiko Sistem Aplikasi EUC

Bank harus mendefinisikan tingkat risiko untuk setiap sistem aplikasi EUC secara periodik. Apabila sistem aplikasi memiliki risiko tinggi maka pengembangan harus dilakukan oleh Satuan Kerja TI termasuk pemeliharannya.

Beberapa risiko yang terkait dengan EUC antara lain:

- a. jika EUC tidak memenuhi standar pengamanan yang memadai, maka terdapat risiko akses oleh pihak yang tidak berwenang yang dapat menyebabkan kebocoran data/informasi serta kejahatan atau kecurangan yang mengakibatkan kerugian finansial maupun non-finansial;
- b. dokumentasi sistem aplikasi yang tidak memadai dapat menyebabkan ketergantungan pada personil yang mengembangkan dan mengetahui sistem (*key person*);
- c. sistem aplikasi yang dikembangkan kurang memadai, antara lain disebabkan karena:
 - 1) kurangnya pemahaman terhadap risiko-risiko yang mungkin ada;
 - 2) kurangnya tingkat kompetensi dan pengalaman pengguna akhir dalam pengembangan sistem aplikasi;
 - 3) penggunaan teknologi tanpa memperhatikan kebutuhan bisnis dan kondisi Bank.
- d. pengembangan dan penggunaan sistem oleh masing-masing satuan kerja pengguna akhir dapat menimbulkan ketidakjelasan mengenai tanggung jawab terhadap kepemilikan sistem, data serta penanganan masalah yang timbul;
- e. menurunnya integritas dan akurasi data/informasi Bank;
- f. tidak tersedia jejak audit (*audit trail*) yang memadai sehingga mengakibatkan keterbatasan kemampuan Bank untuk melakukan penelusuran, seperti apabila terjadi dugaan *fraud*.

Dengan melihat risiko-risiko diatas, EUC harus dilakukan melalui koordinasi antara satuan kerja pengguna dan satuan kerja TI. Pengguna dapat mengembangkan sistem aplikasi sendiri namun satuan kerja TI harus menginventarisir sistem aplikasi tersebut, dan mengevaluasi kesesuaiannya dengan kebijakan dan prosedur pengembangan Bank. Apabila aplikasi serupa diperlukan oleh satuan kerja lain maka dapat implementasikan ke satuan kerja yang memiliki kebutuhan yang sama tersebut. Terdapat beberapa metode pengukuran risiko yang dapat dipergunakan oleh Bank. Apabila Bank menggunakan *Control Self Assessment* (CSA) dalam menilai risiko, maka Bank harus memasukkan EUC kedalam ruang lingkup CSA yang dilakukan masing-masing satuan kerja. Setiap Bank dapat menetapkan sendiri kriteria risiko (*risk-appetite*) disesuaikan dengan skala dan kondisi Bank yang bersangkutan. Contoh pengkategorian tingkat risiko dapat dilihat pada lampiran 1.2.

7.4.2. Pengendalian dan Mitigasi Risiko

Mengingat risiko-risiko yang terdapat pada sistem aplikasi EUC sebaiknya pengembangan dan penggunaan sistem aplikasi EUC hanya dilakukan apabila kebutuhan pengguna begitu mendesak, detail, beragam, dan/atau penggunaan sistem aplikasi tersebut bersifat sementara. Disamping itu Bank harus senantiasa melakukan pengendalian yang memadai pada EUC. Bentuk-bentuk pengendalian yang harus diterapkan Bank mencakup paling kurang sebagai berikut:

- a. Pengendalian pada pengembangan, pengujian dan perubahan aplikasi EUC antara lain:
 - 1) setiap aplikasi EUC yang akan dikembangkan harus dilaporkan kepada Satuan Kerja TI;
 - 2) Satuan Kerja TI harus memberikan persetujuan/sertifikasi sebelum aplikasi tersebut dapat digunakan oleh satuan kerja pengguna. Persetujuan diberikan setelah terlebih dahulu dilakukan analisis kecukupan aplikasi dari sisi fungsional, pengamanan (fisik dan logik), serta kesesuaian aplikasi dengan kebutuhan pengguna;
 - 3) Satuan Kerja TI harus menginventarisasi seluruh aplikasi EUC yang digunakan unit pengguna, termasuk setiap penambahan atau modifikasi yang ada;
 - 4) dalam hal terdapat penambahan atau modifikasi terhadap aplikasi maka pengguna harus melaporkan ulang dan mendapat persetujuan dari satuan kerja TI sebagaimana dimaksud dalam huruf a dan b;
 - 5) untuk menghindari dan melindungi kerahasiaan program dan data dari pihak yang tidak berwenang, Bank harus memiliki tindakan pengamanan terhadap data, *source code* dan *executable file*.

Selain itu, Bank juga perlu mempertimbangkan kaidah-kaidah umum pengendalian pengembangan aplikasi sebagaimana diatur dalam Bab II *Development & Acquisition*.

- b. Standar pengamanan pada setiap aplikasi EUC dengan mengacu kepada Kebijakan Pengamanan Informasi sebagaimana dimaksud pada Bab V. Pengamanan Informasi yang diperlukan untuk meminimalkan risiko operasional. Standar tersebut paling kurang mencakup hal-hal sebagai berikut:
 - 1) proses validasi diperlukan dalam melakukan input data ke aplikasi EUC secara manual maupun transmisi antar-komputer (*download*, *upload* atau transfer secara elektronik) melalui suatu jaringan untuk menjamin integritas data;
 - 2) pengendalian yang memadai pada tahap persiapan data, pelaksanaan input, pemrosesan, distribusi output, dan proses rekonsiliasi perlu ditetapkan oleh Bank. Hal ini diterapkan terutama pada aplikasi EUC yang digunakan untuk memproses informasi keuangan Bank atau nasabah karena harus memperhatikan terjaminnya integritas data dan tersedianya *audit trail*;

- 3) manajemen Bank perlu melakukan *backup* data dan aplikasi EUC secara periodik. Selain itu DRP dan BCP Bank harus memperhitungkan risiko yang terkait dengan aplikasi EUC.

7.5. AUDIT INTERN

Hal-hal yang perlu diperhatikan oleh Bank berkaitan dengan audit terhadap aplikasi EUC, antara lain:

- a. aplikasi EUC tersebut termasuk obyek pemeriksaan satuan kerja audit intern TI;
- b. audit dilakukan secara berkala untuk memastikan bahwa pengendalian yang diterapkan memadai dan efektif;
- c. Bank harus memastikan terdapat tindak lanjut atas temuan hasil pelaksanaan audit.

BAB VIII

ELECTRONIC BANKING

8.1. PENDAHULUAN

Perkembangan pesat Teknologi Informasi (TI) dan globalisasi mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman dan efektif, diantaranya melalui media elektronik atau dikenal dengan *e-banking*. Melalui *e-banking*, nasabah Bank pada umumnya dapat mengakses produk dan jasa perbankan dengan menggunakan berbagai peralatan elektronik (*intelligent electronic device*) seperti *personal computer* (PC), *personal digital assistant* (PDA), anjungan tunai mandiri (ATM), kios, atau *telephone*.

Dalam pedoman ini yang dimaksud dengan *Electronic Banking* (*e-banking*) adalah layanan yang memungkinkan nasabah Bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti Automatic Teller Machine (ATM), *phone banking*, *electronic fund transfer* (EFT), *Electronic Data Capture* (EDC)/*Point Of Sales* (POS), *internet banking* dan *mobile banking*. Dalam memberikan pelayanan *e-banking*, Bank dapat menyediakan layanan yang bersifat *informational*, *communicative* dan/atau *transactional*. Penyediaan layanan *e-banking* hendaknya memperhatikan prinsip *prudential banking*, prinsip pengamanan dan terintegrasinya sistem TI, *cost effectiveness*, perlindungan nasabah yang memadai serta searah dengan strategi bisnis Bank.

Mengingat *e-banking* hanya merupakan *alternative delivery channel* maka selain menghadapi risiko yang telah ada, terdapat juga penambahan dan peningkatan risiko operasional, risiko hukum dan risiko reputasi yang berasal dari penggunaan Teknologi Informasi.

8.2. PERAN DAN TANGGUNG JAWAB MANAJEMEN

Komisaris dan Direksi harus melakukan pengawasan yang efektif terhadap risiko yang terkait dengan aktivitas *e-banking*, termasuk penetapan akuntabilitas, kebijakan, dan proses pengendalian untuk mengelola risiko tersebut.

8.2.1. Dewan Komisaris

- a. Komisaris harus mengarahkan kebijakan yang terkait dengan rencana aktivitas *e-banking* dan mengevaluasi kesesuaian rencana tersebut dengan rencana strategis Teknologi Informasi Bank dan rencana strategis bisnis;
- b. Komisaris harus melakukan pengawasan terhadap pelaksanaan kebijakan yang terkait dengan aktivitas *e-banking*.

8.2.2. Direksi

- a. Direksi harus melakukan kaji ulang terhadap rencana pelaksanaan *e-banking* yang berpotensi memiliki dampak yang signifikan terhadap strategi dan profil risiko Bank termasuk analisa *cost* dan *benefit* dari rencana *e-banking* tersebut;
- b. Direksi harus memastikan bahwa Bank pada saat memasuki aktivitas *e-banking* telah memiliki manajemen risiko yang memadai. Selain itu Direksi harus memastikan bahwa pejabat atau pegawai yang terkait dengan aktivitas *e-banking* memiliki kompetensi dalam aplikasi dan teknologi pendukung *e-banking*;
- c. Direksi harus melakukan pemantauan secara berkala terhadap risiko-risiko yang melekat pada *e-banking*, dan melaporkan hasil pemantauan tersebut kepada Komisaris;
- d. Direksi harus memastikan bahwa proses Manajemen Risiko aktivitas *e-banking* terintegrasi dalam Manajemen Risiko Bank secara keseluruhan. Kebijakan dan prosedur manajemen risiko harus dievaluasi untuk mengantisipasi risiko tambahan yang berasal dari aktivitas *e-banking*. Untuk itu Bank perlu melakukan langkah-langkah sebagai berikut:
 - 1) menetapkan limit risiko dalam kaitannya dengan *e-banking* dengan memperhatikan *risk appetite* Bank;
 - 2) menetapkan delegasi wewenang dan mekanisme pelaporan, termasuk prosedur yang diperlukan untuk kejadian yang berdampak pada kondisi keuangan dan reputasi Bank;
 - 3) memperhatikan faktor-faktor risiko yang secara khusus berhubungan dengan keamanan, integritas dan ketersediaan jasa *e-banking*;
 - 4) memastikan bahwa uji tuntas (*due dilligence*) dan analisis risiko yang memadai telah dilaksanakan sebelum Bank melakukan aktivitas *e-banking* transaksional secara *cross border*.
- e. Dalam hal sistem penyelenggaraan *e-banking* dilakukan oleh pihak lain (*outsourcing*), Bank harus menetapkan dan menerapkan prosedur pengawasan dan *due dilligence* yang menyeluruh dan berkelanjutan untuk mengelola hubungan Bank dengan pihak lain tersebut;
- f. Dalam melakukan kaji ulang terhadap aspek utama prosedur pengendalian pengamanan Bank, direksi harus:
 - 1) mengawasi pengembangan dan pemeliharaan yang berkesinambungan atas infrastruktur pengendalian pengamanan yang melindungi sistem *e-banking* dan data Bank dari gangguan internal dan eksternal;
 - 2) memastikan bahwa Bank memiliki kebijakan dan prosedur pengendalian pengamanan yang menyeluruh untuk menangani potensi ancaman pengamanan yang berasal dari intern dan ekstern, baik dalam bentuk tindakan pencegahan maupun penanganan insiden tersebut. Prosedur pengendalian pengamanan tersebut diantaranya meliputi:

- a) adanya penugasan terhadap pejabat Bank yang bertanggung jawab untuk mengawasi penyusunan dan pemeliharaan kebijakan pengamanan Bank (*corporate level security policy*);
 - b) pengendalian fisik yang memadai untuk mencegah *unauthorized physical access* terhadap ruang komputer;
 - c) prosedur pengendalian logik dan pemantauan yang memadai untuk pengujian keaslian identitas pengguna sehingga mencegah *unauthorized access* internal dan eksternal terhadap aplikasi dan *database* transaksi *e-banking*;
 - d) kaji ulang dan pengujian secara berkala terhadap langkah-langkah pengamanan sistem yang digunakan untuk *e-banking*.
- 3) memastikan diterapkannya manajemen risiko oleh satuan kerja TI dan satuan kerja operasional *e-banking*. Antara lain dilaksanakannya *self assessment* berupa mengukur dan memantau risiko terkait kegiatan *e-banking* dan digunakannya hasil *self assessment* tersebut dalam kebijakan dan prosedur yang ditetapkan Bank untuk pengamanan risiko-risiko pada *e-banking*.

8.3. KEBIJAKAN DAN PROSEDUR (*POLICY & PROCEDURES*)

Dalam rangka pengelolaan risiko yang melekat pada produk dan aktivitas *e-banking*, Bank harus memiliki kebijakan dan prosedur secara tertulis untuk setiap produk *e-banking* yang diterbitkannya paling kurang:

- a. prosedur pelaksanaan (*standard operating procedures*) produk dan aktivitas *e-banking*;
- b. tanggung jawab dan kewenangan dalam pengelolaan produk dan aktivitas *e-banking*;
- c. sistem informasi akuntansi produk *e-banking* termasuk keterkaitan dengan sistem informasi akuntansi Bank secara menyeluruh;
- d. prosedur pengidentifikasian, pengukuran dan pemantauan berbagai risiko yang melekat pada produk *e-banking*.

Setiap prosedur pelaksanaan (*standard operating procedures*) produk harus memenuhi prinsip pengendalian pengamanan data nasabah dan transaksi *e-banking* yaitu:

- a. kerahasiaan (*confidentiality*);
- b. integritas (*integrity*);
- c. ketersediaan (*availability*);
- d. keaslian (*authentication*);
- e. *non repudiation*;
- f. pemisahan tugas dan tanggung jawab (*segregation of duties*);
- g. pengendalian otorisasi dalam sistem, *database* dan aplikasi (*authorization of control*);
- h. pemeliharaan jejak audit (*maintenance of audit trails*).

Dalam menetapkan pengendalian pengamanan pada aktivitas dan produk *e-banking*, Bank hendaknya selain memperhatikan pengamanan layanan terhadap nasabah juga memperhatikan pihak lain yang terkait dengan layanan *e-banking*.

8.4. MANAJEMEN RISIKO AKTIVITAS DAN PRODUK E BANKING

8.4.1. Penilaian Risiko Terkait *E-Banking*

Bank harus melakukan identifikasi atas jenis-jenis risiko yang dapat ditimbulkan oleh aktivitas *e-banking* baik dari produk itu sendiri maupun dari penggunaan Teknologi Informasi sebagai akibat digunakannya *electronic delivery channel*.

Pengukuran dilakukan terhadap setiap kerugian yang terjadi (*loss event*) pada setiap jenis produk. Untuk dapat memantau besar dan kecenderungan risiko dari setiap jenis produk, maka Bank harus membuat *database* yang berisi data historis dari kerugian (*loss event database*) setiap jenis produk.

8.4.1.1. Risiko Umum

Risiko umum meliputi:

- a. *Transaction/Operations Risk*: 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. Termasuk dalam risiko transaksi ini adalah risiko yang dapat timbul dari kurang memadainya pelaksanaan prinsip pengendalian pengamanan tersebut di atas;
- b. *Credit Risk*: risiko kredit dapat timbul apabila Bank memberikan kredit melalui media elektronik misalnya produk kartu kredit;
- c. *Compliance/Legal Risk* yang timbul dari:
 - 1) ketidakpatuhan terhadap hukum dan atau peraturan dari otoritas pengawas;
 - 2) perbedaan dengan hukum di negara lain dalam hal *cross border transaction*;
 - 3) ketidakpatuhan terhadap ketentuan tentang kerahasiaan data nasabah dan ketentuan tentang transparansi informasi produk;
 - 4) keterbatasan ketentuan perundangan sebagai dasar hukum transaksi *e-banking*.
- d. *Strategic Risk* dapat timbul dari:
 - 1) ketidaksesuaian dengan tujuan/rencana bisnis Bank;
 - 2) kurang baiknya perencanaan investasi pada *e-banking* dapat menyebabkan tidak optimalnya *return on investment* yang diperoleh dibandingkan dengan biaya yang dikeluarkan;
 - 3) kurang optimalnya pengelolaan hubungan dengan pihak penyedia jasa TI (*relationship management*);
- e. *Reputation Risk*: risiko reputasi timbul dari kemungkinan menurunnya atau hilangnya kepercayaan nasabah karena *service level delivery* kepada nasabah tidak

terjaga seperti kelambatan atau tidak tersedianya layanan *e-banking*, kelambatan respon atas komplain nasabah, ketidakamanan sistem dan adanya gangguan pada sistem.

- f. *Market Risk*: risiko yang timbul dalam hal Bank membuat produk yang memiliki fitur yang memungkinkan dieksekusinya transaksi yang terekspos perubahan tingkat bunga, perubahan kurs seperti misalnya pada layanan transfer di *internet banking* dari rekening rupiah milik nasabah ke rekening valas tertuju di luar negeri.
- g. *Liquidity Risk*: risiko yang timbul dalam hal Bank tidak membatasi jumlah yang dapat ditransfer oleh nasabah korporasi melalui *internet banking*.

8.4.1.2. Risiko Spesifik

Dalam melaksanakan aktivitas *e-banking*, Bank akan menghadapi risiko spesifik akibat penyediaan dan penggunaan Teknologi Informasi. Risiko ini akan meningkatkan eksposur risiko yang dihadapi Bank. Contoh risiko spesifik yang dihadapi antara lain:

- a. Risiko operasional yang mungkin timbul dari transaksi *e-banking* diantaranya adalah kecurangan, penyadapan/*skimming*, kesalahan, kerusakan atau tidak berfungsinya sistem;
- b. Risiko yang mungkin timbul dari transaksi *cross border e-banking* antara lain risiko hukum mengingat transaksi melewati batas wilayah hukum yang berbeda. Risiko ini timbul karena terdapat perbedaan ketentuan perundangan diantara kedua wilayah hukum, seperti ketentuan perlindungan konsumen, kerahasiaan Bank dan data pribadi nasabah, persyaratan pelaporan dan ketentuan tentang *money laundering*. Selain itu Bank dapat juga menghadapi risiko lain seperti risiko operasional, risiko kredit dan risiko pasar;
- c. Risiko dalam penyelenggaraan *internet banking* meliputi:
 - 1) nasabah memperoleh informasi yang salah atau tidak akurat melalui internet;
 - 2) pencurian data finansial dari *database* Bank melalui *informational* dan *communicative internet banking* yang tidak terisolasi;
 - 3) terdapat ancaman/serangan misalnya *defacing*, *cybersquatting*, *denial of service*, penyadapan komunikasi internet (*network interception*), *man-in-the middle-attack*, virus.
 - 4) terjadi pencurian identitas (*identity theft*) misalnya *phising*, *key logger*, *spoofing*, *cybersquatting*;
 - 5) terjadi transaksi yang dilakukan oleh pihak yang tidak berwenang (*unauthorized transaction*) atau terjadi *fraud*.
- d. Ancaman keamanan pada produk yang menggunakan teknologi *wireless* misalnya *mobile banking* antara lain intrusi atau penyadapan komunikasi akibat belum semua transaksi melalui *mobile banking* dienkripsi, *denial of service attack*, virus, *worm*, *Trojan*, penggandaan *sim card* dan nomor *handphone*;

- e. Ancaman keamanan pada produk *phone banking* yaitu sangat rentan terhadap penyadapan.

8.4.2. Mitigasi Risiko

Bank harus melakukan mitigasi atas risiko umum dan risiko spesifik yang mungkin terjadi dalam layanan *e-banking* dengan memperhatikan prinsip pengendalian pengamanan data nasabah dan transaksi *e-banking*.

8.4.2.1. Prinsip-Prinsip Pengendalian Pengamanan Atas Aktivitas E-Banking

- a. Bank harus melakukan langkah-langkah yang memadai untuk menguji keaslian (*authentication*) identitas dan kewenangan (*authorisation*) nasabah yang melakukan transaksi melalui *e-banking* dengan memperhatikan hal-hal sebagai berikut:
 - 1) Bank harus memiliki kebijakan dan prosedur tertulis untuk memastikan bahwa Bank mampu menguji keaslian identitas dan kewenangan nasabah.
 - 2) Bank dapat menggunakan berbagai metode untuk menguji keaslian yang didasarkan atas penilaian manajemen risiko aktivitas *e-banking*, sensitivitas dan nilai data yang disimpan. Dalam menggunakan metode pengujian keaslian, hendaknya memperhatikan hal-hal sebagai berikut:
 - a) menerapkan kombinasi sekurang-kurangnya 2 faktor otentikasi (*two factor authentication*) yaitu “*what you know*” (*PIN, password*), “*what you have*” (*kartu magnetis dengan chip, token, digital signature*), “*something you are*” atau “*biometric*” (*retina, sidik jari*);
 - b) persyaratan jumlah karakter minimum PIN. Khusus untuk PIN yang digunakan dalam alat pembayaran dengan menggunakan kartu, *mobile banking* dan *internet banking*, panjang PIN harus sekurang-kurangnya terdiri dari 6 digit karakter;
 - c) adanya batasan maksimum kesalahan memasukkan PIN untuk menghambat upaya akses secara tidak sah/legal;
 - d) Bank harus memastikan penerapan prinsip kehati-hatian dalam penggunaan metode pengujian keaslian yang meliputi:
 - (1) pembuatan, validasi dan enkripsi PIN dan metode pengujian keaslian lainnya harus menggunakan metode yang diyakini aman;
 - (2) *database* pengujian keaslian yang menyediakan akses kepada rekening nasabah pada *e-banking* dilindungi dari gangguan dan perusakan;
 - (3) setiap penambahan, penghapusan atau perubahan *database* pengujian keaslian telah dengan tepat diotorisasi oleh pihak yang berwenang;
 - (4) khusus untuk layanan *e-banking* dengan menggunakan kartu, fungsi pembuatan dan pengiriman PIN harus terpisah dari fungsi pembuatan dan pengiriman kartu;

- (5) terdapat sarana pengendalian yang tepat terhadap sistem *e-banking* sehingga pihak ketiga yang tak dikenal tidak bisa menggantikan nasabah yang telah dikenal;
 - (6) terdapat kebijakan yang menyatakan bahwa jika terdapat indikasi telah terjadi pencurian data yang terkait dengan aspek otentikasi nasabah maka Bank wajib melakukan penggantian data otentikasi nasabah dimaksud secepatnya.
- b. Bank harus menyusun dan menetapkan prosedur untuk menjamin bahwa transaksi tidak dapat diingkari oleh nasabah (*non repudiation*) sehingga transaksi dapat dipertanggungjawabkan (kredibel), yang meliputi antara lain:
- 1) sistem *e-banking* telah dirancang untuk mengurangi kemungkinan dilakukannya transaksi secara tidak sengaja (*unintended*) oleh para pengguna yang berhak;
 - 2) seluruh pihak yang melakukan transaksi telah diuji keasliannya;
 - 3) 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 (*logged*) dan menjadi perhatian manajemen Bank;
 - 4) penerapan metode untuk menjamin dipenuhinya prinsip *non repudiation*, misalnya *digital signature*, *Public Key Infrastructure (PKI)*. Kunci-kunci (*keys*) yang digunakan untuk keperluan enkripsi harus dipelihara secara aman sehingga tidak ada satu orang pun yang secara utuh mengetahui kombinasi kunci-kunci tersebut.
- c. Bank harus memastikan terdapat pemisahan tugas dan tanggung jawab terkait penggunaan sistem, *database* dan aplikasi *e-banking*. Bank harus memastikan terdapat *dual control* dan *segregation of duties* untuk memastikan terlaksananya fungsi *check & balance*. Bank perlu memastikan terdapat pemisahan tugas antara pihak yang menginisiasi/menginput data dan pihak yang bertanggung jawab untuk memverifikasi kebenaran data tersebut. Misalnya, dalam suatu aplikasi perbankan, setiap penambahan atau perubahan *database* yang dilakukan oleh *data entry operator*, baru dapat menjadi efektif hanya jika telah disetujui oleh penyeliaanya.
- d. Bank harus memastikan adanya pengendalian terhadap otorisasi dan hak akses (*privileges*) yang tepat terhadap sistem, *database* dan aplikasi *e-banking*. 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.
- e. Bank harus memastikan metode dan prosedur diterapkan untuk melindungi integritas data, catatan dan informasi terkait transaksi *e-banking* dengan memperhatikan hal-hal sebagai berikut:

- 1) Bank harus menerapkan metode dan teknik yang tepat untuk mengurangi ancaman eksternal seperti serangan *virus*, *malicious transaction* yang meliputi:
 - a) perangkat lunak – penyediaan *virus scanning* dan anti virus untuk seluruh *entry point* dan masing-masing sistem komputer (*desktop*);
 - b) perangkat lunak untuk mendeteksi adanya penyusupan (*intrusion detection system*);
 - c) pengujian penetrasi (*penetration testing*) terhadap jaringan internal dan eksternal secara berkala sekurang-kurangnya 1 tahun sekali.
 - 2) Bank harus melakukan pengujian integritas data transaksi *e-banking*.
 - 3) Bank harus melakukan pengendalian/kontrol untuk memastikan seluruh transaksi telah dilaksanakan dengan benar.
- f. Bank harus memastikan tersedianya mekanisme penelusuran (*audit trail*) yang jelas untuk seluruh transaksi *e-banking*, yang mencakup hal-hal sebagai berikut:
- 1) Bank harus memelihara *log* transaksi sesuai kebijakan retensi data Bank sesuai ketentuan perundangan yang berlaku guna tersedianya jejak audit yang jelas serta membantu penyelesaian perselisihan. Data transaksi yang diperlukan perlu mencakup sekurang-kurangnya data nasabah, nomor rekening, jenis transaksi, waktu, lokasi, 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;
 - 3) Bank harus memastikan tersedianya fungsi jejak audit (*audit trail*) untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan yang harus di-*review* 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;
 - 4) Bank harus melakukan pendeteksian dan monitoring atas transaksi yang tidak sah/tidak wajar misalnya melalui *Intrusion Detection System (IDS)* dan *Fraud Detection*. Selanjutnya Bank harus memiliki prosedur penanganan masalah atau kejahatan yang terdeteksi.
- g. Bank harus menerapkan langkah-langkah untuk melindungi kerahasiaan informasi *e-banking*. Prosedur pengamanan disesuaikan dengan tingkat sensitivitas informasi. Bank juga harus memiliki standar dan pengendalian atas penggunaan dan perlindungan data apabila pihak penyedia jasa/*outsourcing* memiliki akses terhadap data tersebut;
- h. Bank harus memiliki *business continuity plan* termasuk *contingency plan* yang efektif untuk memastikan tersedianya sistem dan jasa *e-banking* secara berkesinambungan. Pengaturan lebih lanjut dapat dilihat pada Bab VI tentang *Business Continuity Plan*;

- i. Bank harus mengembangkan rencana penanganan kejadian (*incident response plans*) yang cepat dan tepat untuk mengelola, mengatasi, dan meminimalkan dampak suatu insiden, *fraud*, kegagalan sistem (internal dan eksternal), yang dapat menghambat penyediaan sistem dan jasa *e-banking*.

8.4.2.2. Prinsip Pengendalian Pengamanan Produk *E-Banking* Tertentu

- a. Dalam menyediakan layanan jasa perbankan melalui *e-banking* misalnya pada ATM dan *internet banking*, Bank juga harus memperhatikan kenyamanan dan kemudahan nasabah menggunakan fasilitas termasuk efektivitas menu tampilan layanan *e-banking*, khususnya dalam melakukan pilihan pesan yang diinginkan nasabah agar tidak terjadi kesalahan dan kerugian dalam transaksi;
- b. Jika diperlukan untuk meningkatkan pengamanan, Bank dapat menetapkan persyaratan atau melakukan pembatasan transaksi melalui *e-banking* untuk menjamin keamanan dan kehandalan transaksi misalnya meminta nasabah melakukan registrasi rekening pihak ketiga tujuan transfer dalam *mobile banking* atau membatasi nominal jumlah transaksi melalui ATM dan *internet banking*;
- c. Dalam penyelenggaraan layanan *e-banking* yang menyediakan sarana fisik seperti ATM, Bank harus melakukan pengendalian pengamanan fisik terhadap peralatan dan ruangan yang digunakan terhadap bahaya pencurian, kerusakan dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Bank harus melakukan pemantauan secara rutin untuk menjamin keamanan dan kenyamanan bagi nasabah pengguna jasa *e-banking*;
- d. 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 kualitas serta akurasi kinerja perangkat jaringan dan saluran transmisi, pemantauan terhadap akses perangkat lunak *Controller (Host-Front End)*;
- e. *Point of Sales* (POS)/*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*, 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 meminimalkan kemungkinan adanya penyadapan baik di POS Terminal sendiri maupun dalam jaringan komunikasinya.

- f. Bagi Bank yang menyediakan jasa *mobile banking (m-banking)*, maka Bank harus memastikan keamanan transaksi tersebut yang dapat dilakukan antara lain melalui hal-hal sebagai berikut:
- 1) menggunakan suatu *SIM Toolkit* dengan fitur enkripsi *end-to-end* dari *handphone* hingga *server m-banking*, untuk melindungi pengiriman data pada *m-banking*;
 - 2) melakukan *mutual authentication* yaitu pihak Bank dan nasabah dapat melakukan proses otentifikasi dengan *digital certificate*, *Personal Authentication Message* yaitu untuk membantu nasabah memastikan bahwa pihak yang bertransaksi dengan nasabah adalah pihak yang benar (Bank, penyedia jasa).
- g. Dalam penyediaan jasa layanan *phone banking*, Bank harus memastikan keamanan transaksi diantaranya melalui hal-hal sebagai berikut:
- 1) layanan ini tidak digunakan untuk transaksi dengan nilai maupun risiko yang tinggi;
 - 2) semua percakapan melalui IVR direkam termasuk nomor telepon nasabah, detil transaksi, dll;
 - 3) layanan ini menggunakan metode otentifikasi yang handal dan aman;
 - 4) penggunaan metode otentifikasi nasabah seperti PIN dan *password* untuk transaksi finansial.

8.4.2.3. Edukasi dan Perlindungan Nasabah

Bank wajib melakukan edukasi nasabah agar setiap pengguna jasa layanan Bank melalui *e-banking* menyadari dan memahami risiko yang dihadapinya. Hal-hal yang harus dilakukan Bank antara lain meliputi:

- a. untuk transaksi *internet banking*, Bank harus memastikan bahwa *website* Bank telah menyediakan informasi yang memungkinkan calon nasabah memperoleh informasi yang tepat mengenai identitas dan status hukum Bank sebelum melakukan transaksi. Informasi tersebut mencakup namun tidak terbatas pada: nama dan tempat kedudukan Bank, identitas otoritas pengawasan Bank, tata cara nasabah mengakses unit pelayanan nasabah (*call center*) dan tata cara bagi nasabah untuk mengajukan pengaduan;
- b. apabila Bank memperbolehkan nasabah untuk membuka rekening melalui internet, maka harus terdapat informasi pada *website* Bank tentang ketentuan hukum terkait *Know Your Customer* diantaranya nasabah harus datang dan mengikuti prosedur wawancara;
- c. Bank harus memastikan bahwa perlindungan terhadap kerahasiaan data nasabah diterapkan sesuai dengan ketentuan yang berlaku dan hanya dapat diakses oleh pihak yang memiliki kewenangan. Selain itu hendaknya nasabah diberikan pemahaman mengenai peraturan intern Bank mengenai kerahasiaan data nasabah;

- d. Bank harus memastikan bahwa data nasabah tidak digunakan untuk tujuan di luar otorisasi yang diberikan oleh nasabah. Sesuai ketentuan yang berlaku mengenai transparansi informasi produk dan penggunaan data pribadi nasabah, Bank harus memperoleh izin nasabah apabila hendak memberikan data pribadi nasabah kepada pihak penyedia jasa untuk keperluan *marketing*. Perlindungan terhadap kerahasiaan data nasabah juga harus dipenuhi dalam hal Bank menggunakan jasa pihak lain (*outsourcing*);
- e. edukasi yang diberikan kepada nasabah mencakup tentang hak, kewajiban dan tanggung jawab seluruh pihak terkait. Edukasi sekurang-kurangnya diberikan pada saat nasabah mengajukan aplikasi pelayanan *e-banking*.

Hal-hal yang perlu diedukasikan antara lain:

- 1) pentingnya menjaga keamanan PIN/*Password* misalnya:
 - a) merahasiakan dan tidak memberitahukan PIN/*Password* kepada siapapun termasuk kepada petugas Bank;
 - b) melakukan perubahan secara berkala;
 - c) menggunakan PIN/*Password* yang tidak mudah ditebak (penggunaan identitas pribadi seperti tanggal lahir);
 - d) tidak mencatat PIN/*Password*;
 - e) PIN untuk satu produk hendaknya berbeda dari PIN produk lainnya.
- 2) penerapan prinsip kehati-hatian saat menggunakan ATM antara lain:
 - a) memperhatikan keamanan lingkungan tempat ATM sebelum memutuskan untuk mengambil uang;
 - b) memastikan uang dan kartu telah diambil sebelum meninggalkan lokasi ATM.
- 3) penyediaan informasi kepada nasabah mengenai teknik pengamanan komputer pribadi nasabah yang digunakan dalam *internet banking*.
- 4) prosedur pengaduan jika terjadi masalah.
- 5) penerapan prinsip kehati-hatian dalam menggunakan mobile banking misalnya:
 - a) tidak menyimpan PIN dalam memori telepon untuk mencegah penggandaan *sim card* secara ilegal maupun pencurian PIN melalui fungsi *redial*;
 - b) menggunakan metode untuk melakukan verifikasi keotentikan dari nasabah dan atau Bank yang menghubungi misalnya dengan menggunakan *personal assurance message* yaitu informasi personal yang disampaikan nasabah kepada Bank saat registrasi sehingga nasabah dan Bank dapat melakukan *verifikasi* saat terjadi transaksi.
- 6) dalam menggunakan *internet banking* diperlukan edukasi mengenai berbagai modus kejahatan *internet banking* seperti:
 - a) *phising* dan kejahatan *social engineering* lainnya;
 - b) *key logger* dan *Trojan Horse Virus* pada berbagai peralatan komputer yang umumnya terdapat di tempat-tempat umum seperti warung Internet (*warnet*), *Internet Cafe*, dll.

8.4.2.4. Cross Border Electronic Banking

Mitigasi terhadap risiko *cross border e-banking* dilakukan dengan cara:

- a. membangun program manajemen risiko yang efektif untuk aktivitas *e-banking* yang melewati batas negara (*cross border*). Sebelum Bank mengenalkan produk dan jasa *cross border e-banking*, manajemen Bank sebaiknya melakukan penilaian risiko dan *due diligence* yang tepat guna menjamin bahwa Bank secara tepat mengelola risiko-risiko yang ada. Selain memperhatikan setiap hukum dan peraturan yang berlaku di Indonesia, Bank hendaknya memperhatikan hukum dan peraturan yang berlaku di negara tempat Bank akan menawarkan jasa *cross border e-banking*.
- b. adanya pengungkapan yang cukup pada *website* atau informasi lainnya guna memungkinkan nasabah potensial sebelum melakukan hubungan bisnis dengan Bank mengetahui identitas Bank, *home country*, otoritas pengawas Bank dan izin yang diperoleh Bank.

8.4.2.5. Pengelolaan Risiko Terkait Sistem dan Layanan E-Banking yang Diselenggarakan oleh Pihak Penyedia Jasa

Dalam hal sistem penyelenggaraan *e-banking* dilakukan oleh pihak lain (*outsourcing*) misalnya *switching company*, ISP, Bank harus menetapkan dan menerapkan prosedur pengawasan dan *due diligence* yang menyeluruh dan berkelanjutan untuk mengelola hubungan Bank dengan pihak penyedia jasa tersebut. Untuk itu Bank harus membuat suatu perjanjian tertulis dengan pihak penyedia jasa terkait layanan *e-banking* yang secara rinci mengatur hak dan kewajiban, aspek pengamanan, dan melakukan pemantauan kinerja pihak penyedia jasa sesuai *service level agreement*. Pengaturan lebih lanjut dapat dilihat pada Bab X – Panduan Penggunaan Penyedia Jasa Teknologi Informasi.

8.5. AUDIT INTERN

Tujuan pelaksanaan audit terhadap aktivitas *e-banking* adalah untuk menguji efektivitas pelaksanaan manajemen risiko atas kegiatan *e-banking* serta memastikan bahwa pengendalian pengamanan produk tersebut telah memadai untuk memberikan perlindungan bagi nasabah. Audit atas aktivitas *e-banking* paling kurang mencakup evaluasi atas pengawasan manajemen (*board and management oversight*), penilaian atas program pengamanan yang diterapkan serta kaji ulang atas kepatuhan terhadap ketentuan perundangan.

Penerapan audit terhadap layanan *e-banking* sekurang-kurangnya mengacu pada Bab IX Audit.

8.6. PELAPORAN RENCANA & REALISASI PRODUK *E-BANKING* BARU

Setiap rencana penerbitan produk *Electronic Banking* yang bersifat transaksional wajib dilaporkan kepada Bank Indonesia paling lambat 2 (dua) bulan sebelum produk tersebut diterbitkan dengan menggunakan Lampiran 2.21. Rencana Penerbitan *Electronic Banking* Transaksional. Ketentuan pelaporan rencana produk *Electronic Banking* berlaku untuk setiap produk baru yang karakteristiknya berbeda dengan produk yang telah ada di Bank dan/atau menambah atau meningkatkan eksposur risiko tertentu pada Bank. Ketentuan pelaporan ini tidak berlaku untuk produk *Electronic Banking* yang diatur secara khusus dalam ketentuan Bank Indonesia mengenai persyaratan persetujuan produk tersebut.

Dalam hal Teknologi Informasi yang digunakan dalam menyelenggarakan kegiatan *Electronic Banking* dilakukan oleh pihak penyedia jasa maka berlaku pula ketentuan penggunaan penyedia jasa sebagaimana diatur dalam Bab X mengenai Penggunaan Pihak Penyedia Jasa Teknologi Informasi.

Yang dimaksud dengan “produk *Elektronik Banking* 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 *phone banking* untuk nasabah penyimpanan.

Dengan demikian apabila Bank hanya menambah jenis layanan pada produk *e-banking* yang telah ada dan penambahan risikonya tidak signifikan misalnya penambahan fasilitas pembayaran melalui *e-banking* 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.

Selanjutnya paling lambat 1 (satu) bulan sejak kegiatan tersebut efektif dioperasikan, Bank wajib melaporkan realisasi kegiatan sesuai format Laporan Perubahan Mendasar dalam Penggunaan Teknologi Informasi dengan menggunakan Lampiran 2.3.1. Realisasi Penerbitan *Electronic Banking* Transaksional. Laporan realisasi tersebut harus dilengkapi dengan tinjauan atas hasil implementasi (*Post Implementation Review*) oleh pihak independen. Produk dan/atau aktivitas baru yang telah dilaporkan dalam Laporan Realisasi Rencana Perubahan Mendasar Teknologi Informasi tidak perlu dilaporkan dalam Laporan Produk dan Aktivitas Baru sebagaimana diatur dalam ketentuan Bank Indonesia mengenai manajemen risiko Bank umum.

8.6.1. Laporan Rencana & Realisasi Produk Baru *E-Banking*

Dalam laporan Rencana Penerbitan *e-banking* transaksional, Bank wajib melampirkan:

- a. bukti-bukti kesiapan untuk menyelenggarakan *e-banking* yang paling kurang mencakup:
 - 1) kesiapan struktur organisasi termasuk pengawasan dari pihak manajemen;
 - 2) kesiapan kebijakan, sistem, prosedur dan kewenangan dalam penerbitan produk *e-banking*;
 - 3) kesiapan infrastruktur TI untuk mendukung produk *e-banking* termasuk namun tidak terbatas pada struktur jaringan, *operating system*, *interface* antara *e-banking system* dan sistem secara keseluruhan;
 - 4) hasil analisis dan identifikasi risiko yang melekat pada produk *e-banking*;
 - 5) kesiapan penerapan manajemen risiko khususnya pengendalian pengamanan (*security control*) atas produk *e-banking* yang memadai yang antara lain untuk memastikan terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), otentikasi (*authentication*), *non repudiation*, dan ketersediaan (*availability*);
 - 6) hasil analisis aspek hukum yang terkait dengan perjanjian antara Bank dengan nasabah serta pihak lain yang mendukung, pemilihan hukum yang digunakan saat terjadi perselisihan/sengketa;
 - 7) uraian sistem informasi akuntansi termasuk penjelasan singkat mengenai keterkaitan dengan sistem informasi akuntansi Bank secara menyeluruh;
 - 8) perlindungan nasabah dan program edukasi nasabah atas sistem dan teknologi pengamanan *e-banking*.
- b. Hasil analisis bisnis mengenai proyeksi produk baru 1 (satu) tahun kedepan sekurang-kurangnya memuat:
 - 1) potensi pasar yang ada;
 - 2) segmen pasar yang akan dituju;
 - 3) analisis persaingan usaha;
 - 4) target nasabah yang ingin dicapai;
 - 5) rencana kerja sama dengan pihak lain;
 - 6) target pendapatan yang akan dicapai.
- c. Hasil pemeriksaan dari pihak independen untuk memberikan pendapat atas karakteristik produk dan kecukupan pengamanan produk serta kepatuhan terhadap ketentuan dan/atau praktek-praktek yang berlaku di dunia internasional.

8.6.1.1. Pemeriksaan oleh Pihak Independen

Hasil pemeriksaan oleh pihak independen sebagaimana dimaksud di atas, ditujukan untuk memberikan pendapat atas karakteristik produk dan kecukupan pengamanan sistem TI terkait produk tersebut serta kepatuhan terhadap ketentuan

dan/atau praktek-praktek yang berlaku (*best practice*) yang memenuhi standar internasional seperti ISO, IEC, COBIT, IT-IL.

Yang dimaksud dengan pihak independen adalah pihak-pihak yang tidak terlibat dalam perancangan dan pengembangan sistem aplikasi serta pengambilan keputusan untuk implementasi (*go or no go*).

Hasil pemeriksaan dari pihak independen di luar Bank (Kantor Akuntan Publik atau perusahaan konsultan dibidang *IT Security* atau sejenisnya) diperlukan untuk produk *e-banking* bersifat transaksional yang baru pertama kali diterbitkan oleh Bank seperti *internet banking* yang bersifat transaksional dan *sms banking* yang bersifat transaksional.

Sedangkan untuk penambahan fitur layanan produk *e-banking* yang telah ada di Bank yang dapat menambah atau meningkatkan eksposur risiko Bank dapat menggunakan pihak internal untuk melakukan *independent review*.

Contoh:

- a. transaksi melalui ATM yang sebelumnya nasabah tidak bisa melakukan pemindahbukuan antar rekening menjadi dapat melakukan pemindahbukuan;
- b. transaksi melalui ATM yang pada mulanya hanya dapat melakukan pemindahbukuan antar rekening dalam Bank kemudian ditambah sehingga dapat melakukan transfer antar Bank.

Bank perlu memastikan bahwa pihak eksternal yang digunakan memiliki kompetensi dan pemahaman terhadap produk yang akan di-*review* terutama dalam aspek pengamanan TI. Dalam hal Bank menggunakan pihak internal untuk melakukan *independent review* maka Bank wajib menyampaikan uraian tugas dan tanggung jawab dari pihak tersebut serta kedudukannya dalam struktur organisasi pada proyek pengembangan aplikasi *e-banking*.

8.6.1.2. Ruang Lingkup Pemeriksaan Pihak Independen

Bank wajib memastikan bahwa laporan yang disampaikan oleh pihak independen mengenai kesiapan TI Bank untuk kegiatan *e-banking* 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 *e-banking* untuk memastikan terpenuhinya prinsip kerahasiaan, integritas, ketersediaan dan *non repudiation* dalam setiap transaksi *e-banking*;
- c. kecukupan penerapan dan pemantauan terhadap pengamanan sistem aplikasi *e-banking* yang disiapkan bank yang meliputi:
 - 1) penerapan pengamanan aplikasi, infrastruktur (*server, firewall* dan *router*) serta jaringan sistem *e-banking*;

- 2) pengamanan untuk mendeteksi transaksi yang tidak wajar;
 - 3) terdapat pemeliharaan dan kaji ulang atas *audit trail log* transaksi;
 - 4) pengamanan fisik yang memadai atas perangkat komputer dan perangkat komunikasi terkait produk/jasa *e-banking*;
 - 5) pengamanan atas jaringan internal bank sehingga terlindung dari serangan yang berasal dari eksternal;
 - 6) pengamanan atas data dan *database* transaksi *e-banking*.
- d. *Business Continuity Plan* dan prosedur tanggap darurat (*incident response management*);
 - e. penggunaan pihak penyedia jasa TI sebagai penyelenggara *e-banking*;
 - f. kaji ulang atas analisis risiko dalam produk baru *e-banking* yang meliputi sekurang-kurangnya risiko strategis, risiko pengamanan, risiko hukum, risiko reputasi;
 - g. program edukasi dan perlindungan nasabah termasuk kehati-hatian dalam pembukaan rekening dan dalam melakukan transaksi melalui *e-banking*.

BAB IX

AUDIT INTERN TEKNOLOGI INFORMASI

9.1. 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 dapat membantu pengurus Bank menjaga aset Bank, menjamin tersedianya pelaporan keuangan dan manajerial yang dapat dipercaya, meningkatkan kepatuhan Bank terhadap ketentuan dan peraturan perundang-undangan yang berlaku, serta mengurangi risiko terjadinya kerugian, penyimpangan dan pelanggaran aspek kehati-hatian.

Penggunaan sarana Teknologi Informasi (TI) disamping meningkatkan kemampuan Bank melaksanakan kegiatan operasional, juga mengandung risiko yang dapat mengakibatkan kerugian, baik yang bersifat finansial maupun non-finansial. Oleh karena itu SPI sangat perlu diterapkan sebagai salah satu upaya meminimalkan kerugian dimaksud. Fungsi audit intern sebagai salah satu bagian dari SPI, bertanggungjawab dalam melakukan evaluasi terhadap penyelenggaraan TI secara independen dan objektif untuk meningkatkan efisiensi dan efektifitas manajemen risiko, pengendalian intern dan tata kelola yang baik.

Pedoman ini dimaksudkan untuk menjadi pedoman minimal bagi Bank dalam melaksanakan audit intern pada bidang TI.

9.2. TUGAS DAN TANGGUNG JAWAB MANAJEMEN

Audit intern Teknologi Informasi merupakan bagian dari Satuan Kerja Audit Intern (SKAI) yang independen dari tugas operasional baik secara organisasi maupun fungsinya. Dalam rangka melaksanakan kegiatannya, audit Intern harus memperoleh dukungan dari manajemen yang diformalkan dalam *Audit Charter*. *Audit Charter* minimal berisikan informasi mengenai kedudukan, tujuan dan ruang lingkup kerja, tugas, wewenang dan tanggung jawab audit Intern. *Audit Charter* tersebut juga memuat pernyataan independensi terhadap kegiatan operasional dari auditee dan pernyataan bahwa setiap aktivitas Bank harus masuk dalam ruang lingkup audit intern Bank.

Keberhasilan audit intern TI memerlukan dukungan Dewan Komisaris, Komite Audit dan Direksi. Ketiga pihak tersebut perlu memastikan kerja sama antara manajemen satuan kerja TI dan manajemen satuan pengguna Teknologi Informasi dengan satuan kerja audit TI. Disamping itu ketiga pihak tersebut perlu pula memastikan bahwa implementasi pengendalian dan pelaksanaan prosedur dan standar dilakukan oleh satuan kerja TI dan satuan kerja pengguna TI. Demikian juga perlu dipastikan bahwa proses audit mencakup upaya verifikasi dan pemantauan

implementasi pengendalian dan pelaksanaan prosedur dan standar secara memadai, tepat waktu dan independen.

9.2.1 Tugas Satuan Kerja Audit Intern

Agar audit intern TI efektif dan dapat menjamin integritas data dan menunjang kelangsungan operasional Bank, SKAI sekurang-kurangnya melakukan beberapa hal berikut:

- a. menyusun dan mengkinikan pedoman kerja yang sekurang-kurangnya mencakup standar baku prosedur pemeriksaan, kertas kerja dan pelaporan hasil pemeriksaan;
- b. mengidentifikasi area risiko TI yang akan menjadi fokus audit;
- c. melakukan evaluasi terhadap fungsi dan kecukupan pengendalian intern dalam sistem informasi Bank;
- d. memastikan penerapan prinsip kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) TI;
- e. mengevaluasi efektifitas perencanaan dan pengawasan penyelenggaraan TI yang dilakukan oleh satuan kerja TI dan satuan kerja pengguna TI;
- f. mengevaluasi kepatuhan TI Bank terhadap ketentuan intern, ketentuan Bank Indonesia dan ketentuan perundang-undangan yang berlaku serta *international best practices* (misalnya ISO, IEC, COBIT, IT-IL, *Capability Maturity Model*);
- g. menyarankan alternatif perbaikan untuk mengatasi kekurangan aspek-aspek terkait TI khususnya di bidang pengamanan;
- h. melakukan pemantauan terhadap tindak lanjut atas hasil audit;
- i. berperan sebagai nara sumber dalam aspek pengendalian dalam hal Bank melakukan pengembangan penyelenggaraan TI seperti pengembangan aplikasi.

9.2.2 Peranan Dewan Komisaris

Tugas utama komisaris terkait penggunaan TI antara lain melakukan evaluasi terhadap perencanaan dan pelaksanaan audit, memastikan audit dilaksanakan dengan frekuensi dan lingkup yang memadai serta melakukan pemantauan atas tindak lanjut hasil audit.

9.2.3 Peranan Direksi

Adapun peran dan tanggung jawab Direktur Utama antara lain:

- a. menetapkan pedoman, sistem dan prosedur audit intern;
- b. memastikan terselenggaranya fungsi audit TI oleh sumber daya yang kompeten dan independen;
- c. memastikan sumber daya manusia pelaksana audit intern TI memadai dan berkualitas serta memperoleh pendidikan dan pelatihan TI yang diperlukan secara berkelanjutan sehingga dapat mengikuti perkembangan TI;
- d. menyetujui rencana audit sebelum dilaksanakan.

9.2.4 Peranan Komite Audit

Peran dan tanggung jawab Komite Audit :

1. melakukan pemantauan dan evaluasi atas perencanaan dan pelaksanaan audit TI yang cukup dengan frekuensi dan lingkup audit yang memadai;
2. pemantauan tindak lanjut hasil audit oleh direksi atas hasil temuan SKAI, akuntan publik dan hasil pengawasan Bank Indonesia.

9.3. PEDOMAN AUDIT TI

Bank perlu memiliki pedoman audit TI tertulis dan disetujui oleh direksi. Kompleksitas pedoman audit TI disesuaikan dengan tujuan, kebijakan usaha, ukuran dan kompleksitas usaha Bank.

Pedoman audit TI antara lain berisi kebijakan dan prosedur yang diperlukan oleh fungsi audit intern TI dan kebijakan dan prosedur pelaksanaan fungsi audit intern oleh pihak lain apabila diperlukan oleh Bank. Pedoman tersebut disamping digunakan sebagai sarana untuk mencapai hasil audit yang efektif dan efisien, juga merupakan pedoman dalam menilai kinerja fungsi audit intern TI. Pedoman tersebut harus memuat kebijakan, prosedur dan standar untuk setiap tahap dalam siklus audit.

9.3.1. Kebijakan Umum Audit

Pedoman audit intern TI paling kurang mencakup kebijakan umum mengenai:

- a. pernyataan visi dan misi fungsi audit intern TI;
- b. struktur organisasi dan sistem pelaporan;
- c. proses penilaian risiko yang menggambarkan risiko inheren di setiap satuan kerja penyelenggara TI dan satuan kerja pengguna TI yang dikinikan secara berkala dan dijadikan dasar untuk perencanaan audit intern TI;
- d. penentuan frekuensi dan jadwal audit yang minimal akan diterapkan Bank untuk audit TI. Audit terhadap penyelenggaraan TI harus direncanakan dan dilaksanakan sekurang-kurangnya 1 (satu) kali dalam setahun terhadap aspek-aspek yang terkait TI sesuai kebutuhan, prioritas dan hasil analisis risiko TI Bank. Sedangkan untuk aplikasi *Core Banking*, keseluruhan modul hendaknya diperiksa oleh audit intern TI sekurang-kurangnya sekali dalam 3 (tiga) tahun;
- e. prosedur audit intern TI untuk setiap aktivitas yang memerlukan audit TI.

9.3.2. Perencanaan Audit

SKAI Bank harus memiliki perencanaan audit tahunan dengan cakupan audit berdasarkan profil risiko pada masing-masing aktivitas terkait TI baik di satuan kerja

TI maupun di satuan kerja pengguna TI. Dalam melakukan penilaian risiko, audit intern TI sekurang-kurangnya melakukan beberapa hal sebagai berikut:

- a. mengidentifikasi data, aplikasi dan sistem operasi, teknologi, fasilitas dan personal;
- b. mengidentifikasi kegiatan dan proses bisnis yang menggunakan TI;
- c. mempertimbangkan skala prioritas berdasarkan dampak dan kemungkinan terjadinya risiko atas kegiatan bisnis terkait dengan TI.

Perencanaan Audit harus mendapat persetujuan dari Presiden Direktur atau Direktur Utama.

9.3.3. Pelaksanaan Audit

Dalam rangka melaksanakan rencana tahunan audit, program audit (*AWP/audit working program*) wajib disusun untuk setiap penugasan audit, yang sekurang-kurangnya mencakup:

- a. organisasi, kewenangan dan tanggung jawab dari auditor;
- b. cakupan audit sesuai hasil penilaian risiko;
- c. tujuan audit, jadwal, jumlah auditor, anggaran dan pelaporan;
- d. outline langkah teknis audit yang diperlukan untuk mencapai tujuan audit.

Dalam pelaksanaan tugasnya, audit intern TI harus memperhatikan aspek-aspek kerahasiaan terhadap data dan informasi yang diperolehnya. SKAI Bank harus memperhatikan fleksibilitas AWP agar dapat disesuaikan dan dilengkapi sesuai dengan risiko yang diidentifikasi.

Temuan audit harus disertai dengan bukti-bukti dan kertas kerja pemeriksaan yang didokumentasikan dengan baik. Untuk itu pedoman audit wajib dilengkapi dengan standar kertas kerja, isi dan format laporan hasil audit, dokumentasi dan distribusi serta pemantauan tindak lanjutnya.

Auditor intern TI perlu berperan dalam pengembangan aplikasi utama, pengadaan, konversi dan testing namun tidak sebagai penentu dapat tidaknya aplikasi yang dikembangkan atau diadakan diimplementasikan, melainkan berpartisipasi sebagai nara sumber dalam aspek pengendalian khususnya mengenai standar pengamanan yang diperlukan. Peran ini diperlukan agar auditor TI dapat menjaga independensi dan obyektifitas dalam pemeriksaan yang akan dilakukan nanti apabila sistem aplikasi telah diimplementasikan.

9.3.4. Pelaporan

Laporan Hasil Audit Intern TI disusun berdasarkan format laporan yang didukung oleh kertas kerja audit yang ditetapkan dalam pedoman audit intern. Laporan tersebut merupakan sarana bagi manajemen untuk membantu melakukan penilaian terhadap kualitas dan kinerja satuan kerja TI, serta memberikan saran perbaikannya. Laporan hasil audit intern TI harus disampaikan kepada satuan kerja yang diperiksa. Disamping itu laporan tersebut disampaikan secara tepat waktu kepada Direktur Utama dan

Dewan Komisaris/Komite Audit dengan tembusan kepada Direktur Kepatuhan. Laporan Hasil Audit Intern TI disampaikan juga kepada Bank Indonesia sebagai bagian dari Laporan Pelaksanaan dan Pokok-Pokok Hasil Audit Intern sebagaimana diatur dalam ketentuan mengenai penerapan standar pelaksanaan fungsi audit intern.

9.3.5. Tindak Lanjut Audit

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

Audit intern harus memelihara dokumentasi atas hasil tindak lanjut tersebut. Laporan tindak lanjut hasil pemeriksaan disampaikan kepada Direktur Utama dan Dewan Komisaris/Komite Audit dengan tembusan kepada Direktur Kepatuhan.

9.4. AUDIT INTERN TI YANG DILAKSANAKAN OLEH PIHAK LAIN

Dalam hal terdapat keterbatasan kemampuan fungsi audit intern atas Teknologi Informasi Bank maka pelaksanaan fungsi audit intern dapat dilakukan oleh auditor ekstern seperti Kantor Akuntan Publik, Lembaga Audit TI Independen atau auditor intern kantor induk bagi bank yang dimiliki bank asing. Penggunaan auditor ekstern untuk melaksanakan fungsi audit intern atas Teknologi Informasi Bank tidak mengurangi tanggung jawab pimpinan Satuan Kerja Audit Intern Bank atas temuan audit dan tindak lanjutnya.

Penggunaan pihak lain sebagai auditor intern TI tersebut wajib mempertimbangkan kompleksitas produk dan skala usaha Bank. Pelaksanaan audit intern TI oleh auditor ekstern tetap memperhatikan aspek kompetensi (antara lain pengetahuan dan pengalaman yang memadai) dan independensi serta didasari dengan suatu kontrak kerja. Meskipun pelaksanaan audit intern diserahkan kepada auditor ekstern namun prosedur audit TI yang dilaksanakan tetap harus mengacu kepada kebijakan dan prosedur audit TI yang dimiliki oleh Bank.

9.5. AUDIT INTERN TERHADAP AKTIVITAS YANG DISELENGGARAKAN OLEH PIHAK LAIN

Agar penggunaan penyedia jasa penyelenggara Teknologi Informasi dapat menunjang kemampuan Bank untuk mengelola bisnisnya secara efektif maka aktivitas tersebut juga merupakan ruang lingkup audit intern Bank. Fungsi audit intern Bank wajib memastikan pengendalian yang dioperasikan oleh pihak penyedia jasa dan melakukan pengujian atas efektivitas pengendalian tersebut. Bank harus memastikan bahwa perjanjian dengan pihak penyedia jasa mencakup klausul penyediaan hak akses bagi

auditor intern Bank dan tidak keberatan untuk diaudit oleh auditor intern Bank. Akses yang disediakan tersebut wajib diberikan baik secara logik maupun phisik.

9.6. KAJI ULANG FUNGSI AUDIT INTERN TI

Bank wajib melakukan kaji ulang atas fungsi audit intern atas penggunaan Teknologi Informasi paling kurang setiap 3 (tiga) tahun sekali. Kaji ulang tersebut wajib menggunakan jasa pihak ekstern yang independen dan bekerja secara independen. Yang dimaksud dengan independen adalah pihak diluar Bank yang tidak memiliki hubungan keuangan, kepengurusan, kepemilikan saham atau hubungan lain yang dapat mempengaruhi kemampuannya untuk bertindak independen. Yang dimaksud dengan bekerja secara independen adalah dapat mengungkapkan pandangan serta pemikiran sesuai dengan profesi, dengan tidak memihak terhadap kepentingan pihak lain.

Kaji ulang yang dilakukan sekurang-kurangnya menilai hasil kerja SKAI dan kepatuhan terhadap ketentuan yang terkait dengan Standar Pelaksanaan Fungsi Audit Intern Bank dan manajemen risiko termasuk manajemen risiko dalam penggunaan teknologi informasi serta ketentuan lainnya. Hasil kaji ulang disertai saran perbaikan dilaporkan kepada Bank Indonesia dan merupakan bagian dari laporan kaji ulang fungsi audit intern (SKAI) sebagaimana diatur dalam ketentuan mengenai penerapan standar pelaksanaan fungsi audit intern.

BAB X

PENGGUNAAN PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI

10.1. PENDAHULUAN

Dalam rangka meningkatkan efektivitas dan efisiensi pencapaian tujuan strategis, Bank dimungkinkan menggunakan pihak penyedia jasa TI. Yang dimaksud dengan menggunakan pihak penyedia jasa teknologi informasi adalah penggunaan jasa pihak lain dalam menyelenggarakan kegiatan Teknologi Informasi yang menyebabkan Bank memiliki ketergantungan terhadap jasa yang diberikan secara berkesinambungan dan atau dalam periode tertentu.

Penggunaan pihak penyedia jasa TI dapat mempengaruhi risiko Bank antara lain risiko operasional, kepatuhan, hukum dan reputasi yang dapat timbul antara lain karena adanya kegagalan penyedia jasa dalam menyediakan jasa, pelanggaran terhadap pengamanan atau ketidakmampuan untuk mematuhi hukum dan peraturan yang berlaku. Untuk memastikan Bank menjalankan usahanya secara sehat dan aman, operasional TI yang dilakukan oleh penyedia jasa TI juga menjadi objek pengaturan dan pengawasan dari otoritas pengawas Bank. Bank Indonesia sebagai otoritas pengawas Bank memiliki kewenangan untuk mengawasi semua aktivitas dan catatan keuangan Bank baik yang dilakukan oleh Bank sendiri atau oleh pihak lain. Untuk itu pemeriksaan dan pengawasan Bank tidak boleh terhambat dengan adanya pengalihan fungsi-fungsi operasional Bank ke pihak lain.

10.2. TANGGUNG JAWAB MANAJEMEN

Manajemen Bank bertanggungjawab penuh terhadap penerapan manajemen risiko atas seluruh aktivitas yang terkait dengan penggunaan pihak penyedia jasa dalam penyelenggaraan TI Bank. Apabila Bank menyerahkan penyelenggaraan TI kepada pihak lain, tanggung jawab akhir (*accountability*) tetap berada pada Bank meskipun *day-to-day responsibility* telah dipindahkan kepada pihak penyedia jasa. Dengan demikian tanggung jawab manajemen tidak hilang atau menjadi berkurang dengan adanya penggunaan penyedia jasa TI. Untuk itu, manajemen Bank wajib mengelola risiko yang ditimbulkan dari kegiatan tersebut secara efektif antara lain dengan:

- a. memahami risiko-risiko secara menyeluruh yang dapat timbul sehubungan dengan penggunaan jasa pihak lain untuk menyelenggarakan sebagian atau keseluruhan operasional TI Bank;

- b. penggunaan pihak penyedia jasa TI memberikan konsekuensi Bank membagi informasi sensitif kepada penyedia jasa, oleh karena itu manajemen wajib melakukan evaluasi kemampuan penyedia jasa untuk menjaga tingkat keamanan paling tidak sama atau lebih ketat dari standar pengamanan Bank. Untuk itu pengawasan dan pemantauan harus dilakukan secara memadai untuk memastikan kecukupan perlindungan terhadap keamanan informasi tersebut;
- c. mengevaluasi calon penyedia jasa berdasarkan cakupan dan faktor kritikal dari jasa yang dikerjakan oleh pihak penyedia jasa;
- d. mempertimbangkan beberapa alternatif pemilihan penyedia jasa yang lain apabila aktivitas yang akan diserahkan penyelenggaraannya kepada pihak penyedia jasa adalah penting;
- e. melakukan kajian dalam rangka menilai kehandalan pihak penyedia jasa baik yang menyangkut kinerja, reputasi penyedia jasa dan kelangsungan penyediaan layanan dalam rangka melakukan pemilihan alternatif-alternatif pihak penyedia jasa Bank;
- f. memastikan Bank memiliki cukup keahlian untuk mengawasi dan mengelola hubungan kerjasama dengan penyedia jasa termasuk menerapkan pengendalian yang efektif;
- g. memastikan setiap hubungan kerja sama dengan penyedia jasa dapat ditangani dengan baik oleh Bank dan dapat memenuhi kebutuhan kegiatan operasional Bank serta sejalan dengan rencana strategis Bank;
- h. memastikan Bank memiliki dokumentasi terkait dengan aktivitas penyediaan jasa TI antara lain prosedur, tugas/tanggungjawab dan mekanisme pelaporan;
- i. melakukan pengawasan secara berkesinambungan atas aktivitas Bank yang dilakukan oleh pihak lain untuk mengatasi risiko yang telah diidentifikasi dan untuk mengevaluasi perubahan-perubahan risiko yang terjadi pada saat pelaksanaan operasional TI dibandingkan dengan pada saat penilaian awal;
- j. melakukan review kontrak/perjanjian secara berkala untuk mengetahui kesesuaian dengan kebutuhan dan kondisi Bank terkini;
- k. khusus untuk penggunaan jasa TI yang memiliki exposure risiko tinggi (berdasarkan hasil *Business Impact Analysis*) seperti penyelenggaraan *Data Center* dan *Disaster Recovery Center*, sebaiknya Bank menggunakan konsultan hukum sejak awal proses rencana penggunaan jasa pihak lain untuk mengkaji proposal yang disampaikan pihak penyedia jasa dan membantu menyiapkan perjanjian agar Bank dapat memahami risiko hukum yang ada dan menerapkan mitigasi risiko yang diperlukan.

Dalam menyerahkan penyelenggaraan TI kepada pihak lain, Direksi bertanggung jawab untuk:

- a. menetapkan kebijakan dan prosedur yang akan digunakan Bank dalam rangka mengevaluasi risiko dan dampak dari penggunaan jasa pihak lain yang ada maupun yang akan digunakan;

- b. mengatur kewenangan persetujuan penggunaan pihak penyedia jasa TI sesuai dengan jenis risiko dan dampaknya;
- c. mengembangkan kebijakan dan prosedur manajemen risiko yang baik dan responsif atas penggunaan jasa pihak ketiga sesuai dengan sifat, cakupan dan kompleksitasnya;
- d. memastikan adanya kaji ulang atas relevansi, keamanan, kehandalan strategi dan kecukupan perjanjian secara berkala.

Dalam menyerahkan penyelenggaraan TI kepada pihak lain, Pejabat Tertinggi TI bertanggung jawab untuk:

- a. menerapkan kebijakan dan prosedur manajemen risiko yang baik dan responsif atas penggunaan jasa pihak ketiga sesuai dengan sifat, cakupan dan kompleksitasnya;
- b. mengkaji ulang keefektifan kebijakan dan prosedur secara berkala;
- c. memastikan bahwa rencana kontinjensi telah disusun dan diuji berdasarkan skenario dengan mempertimbangkan berbagai jenis gangguan;
- d. memastikan adanya kaji ulang dan audit oleh pihak independen terhadap kepatuhan pada kebijakan yang telah dibuat.

10.3. KEBIJAKAN DAN PROSEDUR

10.3.1. Kebijakan Umum

Bank wajib memiliki pedoman mengenai penyelenggaraan TI kepada pihak lain yang sekurang-kurangnya mengatur hal-hal:

- a. standar prosedur pemilihan penyediaan jasa;
- b. standar isi perjanjian kontrak kerja dengan penyedia jasa;
- c. standar sistem pengamanan, akurasi dan integritas terhadap sistem teknologi yang harus dipenuhi oleh penyedia jasa;
- d. pengamanan dan kerahasiaan informasi khususnya informasi nasabah;
- e. evaluasi risiko dan dampak penggunaan jasa pihak lain;
- f. hal-hal lain yang wajib dilakukan Bank dalam penyelenggaraan TI oleh pihak lain sesuai ketentuan yang diatur dalam Peraturan Bank Indonesia tentang Penerapan Manajemen Risiko dalam Penggunaan TI.

10.3.2. Proses Pemilihan Penyedia Jasa

10.3.2.1. Pendefinisian Kebutuhan

Perumusan kebutuhan bisnis akan penggunaan jasa pihak lain wajib dilakukan sebelum Bank memutuskan akan menggunakan jasa pihak lain, diantaranya melalui:

- a. proses pengidentifikasian secara spesifik mengenai fungsi atau aktivitas yang akan diserahkan penyelenggaraannya kepada pihak penyedia jasa;
- 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.

Tahap pendefinisian kebutuhan tersebut diatas harus menghasilkan suatu dokumen yang berisi secara rinci gambaran mengenai harapan Bank terhadap jasa yang akan dikerjakan oleh penyedia jasa. Isi dari dokumen tersebut mencakup beberapa komponen berikut ini:

- a. cakupan dan karakteristik dari layanan, teknologi yang digunakan dan dukungan kepada nasabah;
- b. standar dan tingkat layanan meliputi ketersediaan dan kinerja, *change management*, kualitas layanan, keamanan, kelangsungan usaha;
- c. karakteristik minimal yang harus dipenuhi oleh penyedia jasa yang akan digunakan seperti pengalaman, arsitektur teknologi dan sistem, *process control*, kondisi keuangan, 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 training personil saat transisi atau migrasi ke sistem yang disediakan pihak penyedia jasa;
- f. jangka waktu kontrak, penghentian dan isi minimal dari kontrak;
- g. perlindungan kontrak terhadap kewajiban seperti pembatasan kewajiban dan ganti rugi serta asuransi.

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

10.3.2.2. Permintaan Proposal dari Penyedia Jasa

Proses pemilihan penyedia jasa dimulai dengan permintaan proposal dari penyedia jasa. Proposal yang diajukan harus menjelaskan secara rinci kebutuhan Bank seperti cakupan dan jenis pekerjaan yang akan dilakukan, ekspektasi level jasa produksi, jangka waktu penyelesaian, pengukuran pekerjaan dan pengendaliannya, pengamanan dan kelangsungan bisnis.

Pada saat Bank mengevaluasi proposal, terdapat kemungkinan ditemukannya ketidaksesuaian dengan permintaan Bank. Oleh karena itu Bank harus mengevaluasi perbedaan tersebut dan dampaknya terhadap sasaran dan jasa yang diharapkan Bank. Diantaranya, Bank harus dapat mengkaji kebijakan pihak penyedia jasa yang terkait dengan kepentingan audit penyelenggaraan TI Bank karena akses auditor intern, ekstern maupun Bank Indonesia tidak boleh dikurangi. Dengan demikian data dan informasi yang diperlukan dari penyelenggaraan TI tetap dapat diperoleh secara tepat waktu setiap kali dibutuhkan meskipun TI yang

digunakan Bank tidak diselenggarakan sendiri oleh Bank. Untuk itu surat pernyataan harus termasuk dalam proposal yang disampaikan oleh pihak penyedia jasa. Selanjutnya apabila proposal tersebut telah memenuhi kebutuhan atau sesuai definisi kebutuhan yang telah dibuat Bank maka Bank melakukan negosiasi penyelesaian dengan penyedia jasa sebelum pembuatan kontrak.

10.3.2.3. Due Diligence Penyedia Jasa

Due diligence perlu dilakukan untuk menilai kondisi keuangan, reputasi, kemampuan teknis, kemampuan operasional, strategi pengembangan di masa mendatang, kemampuan untuk mengikuti inovasi di pasar dan mempunyai reputasi yang baik dalam industri perbankan. Dengan demikian Bank mendapatkan keyakinan bahwa penyedia jasa mampu memenuhi kebutuhan Bank. Pada saat *due diligence*, Bank harus melakukan evaluasi dan menilai informasi-informasi yang terkait dengan penyedia jasa yaitu antara lain meliputi:

- a. eksistensi dan sejarah perusahaan;
- b. kualifikasi, latar belakang dan reputasi pemilik perusahaan;
- c. perusahaan lain yang menggunakan jasa yang sama dari penyedia jasa sebagai referensi;
- d. kondisi keuangan termasuk *review* atas laporan keuangan *audited*;
- e. kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual;
- f. teknologi dan arsitektur sistem;
- g. lingkungan pengendalian intern, sejarah pengamanan dan cakupan audit;
- h. kepatuhan terhadap hukum dan ketentuan yang berlaku;
- i. kepercayaan dan keberhasilan dalam berhubungan dengan sub kontraktor;
- j. jaminan asuransi;
- k. kemampuan untuk menyediakan *disaster recovery* dan *business continuity*;
- l. penerapan manajemen risiko;
- m. laporan hasil pemeriksaan pihak independen.

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

10.3.2.4. Penentuan Penyedia Jasa

Dalam menentukan penyedia jasa yang dipilih untuk digunakan oleh Bank dalam menyelenggarakan TI Bank maka Bank harus memperhatikan hal-hal dibawah ini:

- a. oleh karena penggunaan pihak penyedia jasa tidak mengurangi tanggung jawab Bank dalam menerapkan manajemen risiko maka Bank harus melakukan evaluasi atas penerapan manajemen risiko pihak penyedia jasa;
- b. oleh karena Bank harus mampu untuk melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi maka Bank harus memastikan bahwa laporan-laporan yang diperlukan untuk memantau kinerja pihak penyedia jasa telah memadai termasuk bila program pengawasan ternyata diperlukan;
- c. *cost and benefit analysis* yang dilakukan untuk setiap alternatif yang akan dipilih harus mendalam dan memenuhi jangka waktu penggunaan jasa yang direncanakan sesuai Rencana Strategis TI & Rencana Bisnis;
- d. dalam mengkaji setiap alternatif, manajemen Bank harus memastikan satuan kerja Teknologi Informasi di Bank memberikan pendapat dan hasil analisisnya;
- e. pihak penyedia jasa menerapkan prinsip pengendalian TI secara memadai termasuk *physical security* dan *logical security*. Khusus untuk penyelenggaraan *Data Center*, DRC dan Pemrosesan Berbasis TI harus dipastikan bahwa pihak penyedia jasa dapat menyampaikan hasil audit terkini atas Teknologi Informasi yang dilakukan oleh pihak independen;
- f. dalam rangka memantau dan mengevaluasi kehandalan pihak penyedia jasa secara berkala, baik yang menyangkut kinerja, reputasi penyedia jasa dan kelangsungan penyediaan layanan, Bank dapat memperoleh informasi dari berbagai sumber termasuk laporan tahunan pihak penyedia jasa TI tersebut;
- g. Bank harus mempelajari apakah akses terhadap *database* dapat dilakukan oleh Bank Indonesia dapat dilakukan setiap saat baik diperlukan untuk data terkini maupun untuk data yang telah lalu;
- h. apabila pihak penyedia jasa TI merupakan pihak terkait dengan Bank, Bank tetap wajib melakukan proses seleksi. Dokumen penyeleksian harus dapat menunjukkan bahwa pertimbangan-pertimbangan telah dilakukan dengan menganut “hubungan kerja sama secara wajar (*arm's length principle*)”.

10.3.3. Perjanjian Penyediaan Jasa

Setelah memilih sebuah perusahaan penyedia jasa, manajemen membuat perjanjian tertulis dengan penyedia jasa. Isi proposal sebagaimana dipersyaratkan pada proses sebelumnya dapat dijadikan masukan dalam proses ini. Perjanjian merupakan dokumen hukum yang mendefinisikan seluruh aspek dari hubungan dengan pihak penyedia jasa dan menjadi alat kontrol utama.

10.3.3.1. Penyusunan Perjanjian Penyediaan Jasa

Hal-hal minimum yang wajib diatur dalam kontrak antara lain meliputi:

- a. cakupan pekerjaan/jasa;

- b. biaya dan jangka waktu perjanjian kerjasama;
- c. hak dan kewajiban Bank maupun pihak penyelenggara jasa;
- d. jaminan pengamanan dan kerahasiaan data, terutama data nasabah. Data hanya bisa diakses oleh pemilik data (Bank);
- e. *Service Level Agreement (SLA)*, berisi mengenai standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service levels*) dan target kinerja;
- f. harus ditetapkan bahwa SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penyedia jasa;
- g. laporan hasil pemantauan kinerja penyedia jasa yang terkait dengan SLA;
- h. batasan risiko yang ditanggung oleh Bank dan penyedia jasa, diantaranya:
 - 1) risiko perubahan ruang lingkup kontrak;
 - 2) perubahan ruang lingkup bisnis dan organisasi perusahaan penyedia jasa;
 - 3) perubahan aspek hukum serta regulasi;
 - 4) aspek hukum yang meliputi hak cipta, paten dan *trade mark*;
- i. subkontraktor, apabila pihak penyedia jasa melakukan subkontrak sebagian kegiatannya maka persetujuan Bank harus secara tertulis;
- j. tersedianya sarana komunikasi on-line, pengamanan terhadap akses dan transmisi data, dari dan ke Data center, Disaster Recovery Center, dan Pemrosesan Transaksi Berbasis TI;
- k. pengaturan yang jelas mengenai backup, contingency, record protection termasuk hardware, equipment, software dan data files, untuk menjamin kelangsungan penyelenggaraan TI;
- l. pengaturan mengenai pengamanan dalam pengiriman source document yang diperlukan dari dan ke Data center, Disaster Recovery Center, dan Pemrosesan Transaksi Berbasis TI. Pihak yang bertanggungjawab sebaiknya menutup asuransi yang cukup;
- m. kesediaan diaudit baik oleh intern Bank, Bank Indonesia atau pihak ekstern yang ditunjuk oleh Bank maupun oleh Bank Indonesia dan tersedianya informasi untuk keperluan pemeriksaan, termasuk hak akses, baik secara *logic* maupun *physical* terhadap data yang dikelola oleh penyedia jasa;
- n. pihak penyedia jasa wajib memberikan dokumen teknis kepada Bank terkait dengan jasa yang dikerjakan oleh penyedia jasa antara lain alur proses TI dan struktur database;
- o. pihak penyedia jasa harus melaporkan setiap kejadian yang kritis yang dapat mengakibatkan kerugian keuangan dan atau mengganggu kelancaran operasional Bank;
- p. khusus untuk penyelenggaraan Data Center, DRC dan Pemrosesan Berbasis TI, pihak penyedia jasa wajib menyampaikan kepada Bank laporan keuangan terkini yang telah diaudit setiap tahun dan laporan hasil pemeriksaan pihak independen terhadap fasilitas TI yang menjadi obyek perjanjian secara berkala;

- q. tanggung jawab penyedia jasa TI dalam menyediakan sumber daya manusia yang memiliki kualifikasi dan kompetensi sesuai jasa yang disediakan sehingga terjaminnya operasional Bank;
- r. rencana pelatihan sumber daya manusia, baik jumlah yang dilatih, bentuk pelatihan maupun biaya yang diperlukan. Pihak penyedia jasa wajib melakukan transfer knowledge kepada Bank, sehingga terdapat personil satuan kerja Teknologi Informasi di Bank yang memahami TI yang digunakan Bank terutama alur proses TI dan struktur database dari sistem aplikasi yang disediakan oleh pihak penyedia jasa tersebut;
- s. kepemilikan dan hak cipta (license);
- t. garansi bahwa penyedia jasa masih akan mendukung jasa yang diberikan kepada Bank selama periode tertentu setelah implementasi;
- u. pengakhiran/pemutusan kontrak termasuk dalam hal atas permintaan Bank Indonesia;
- v. sanksi dan penalti terhadap alasan-alasan yang tidak jelas terhadap pembatalan kontrak dan pelanggaran isi kontrak;
- w. kepatuhan pada hukum dan ketentuan yang berlaku di Indonesia termasuk penyelesaian jika terjadi perselisihan.

10.3.3.2. Klausula Khusus

Dalam kontrak yang dibuat antara Bank dengan penyedia jasa harus dicantumkan klausula khusus mengenai kemungkinan mengubah, membuat perjanjian baru atau mengambil alih kegiatan yang diselenggarakan oleh pihak penyedia jasa maupun penghentian perjanjian sebelum jangka waktu berakhirnya perjanjian. Termasuk dalam hal ini atas permintaan Bank Indonesia apabila diperlukan dalam rangka pelaksanaan tugas Bank Indonesia selaku otoritas pengawas perbankan. Bank harus mampu mengukur risiko dan efisiensi dari penyelenggaraan TI yang diserahkan kepada pihak penyedia jasa sehingga Bank dapat mengetahui secara dini bila terdapat kondisi-kondisi sebagai berikut:

- a. memburuknya kinerja penyelenggaraan kegiatan Bank oleh pihak penyedia jasa yang dapat berdampak signifikan pada kegiatan usaha Bank;
- b. tingkat solvabilitas pihak penyedia jasa tidak memadai, dalam proses menuju likuidasi atau dipailitkan oleh pengadilan;
- c. terdapat pelanggaran terhadap ketentuan 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 Bank Indonesia.

Bila Bank menemukan hal-hal tersebut diatas maka Bank wajib melakukan hal sebagai berikut:

- a. melaporkan kepada Bank Indonesia paling lambat 3 hari kerja setelah kondisi tersebut di atas diketahui oleh Bank;
- b. memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan jasa apabila diperlukan;
- c. melaporkan kepada Bank Indonesia segera setelah Bank menghentikan penggunaan jasa sebelum berakhirnya jangka waktu perjanjian.

Untuk menjaga kelangsungan usaha Bank dalam hal penghentian penggunaan jasa dilakukan sebelum berakhirnya kontrak maka Bank harus memiliki *contingency plan* yang teruji dan memadai.

10.3.4. Penyedia Jasa Berlokasi di Luar Indonesia

Pada prinsipnya Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* hendaknya diselenggarakan di dalam negeri. Apabila proses dari pendefinisian kebutuhan yang dilakukan oleh Bank sebelum Bank memutuskan akan menggunakan jasa pihak lain ternyata menghasilkan kebutuhan bisnis akan penggunaan jasa pihak lain di luar negeri untuk menyelenggarakan pusat data (*Data Center*) dan *Disaster Recovery Center* maka Bank dapat mempertimbangkan penggunaan jasa pihak lain di luar negeri. Satu hal yang harus dipahami oleh Bank-Bank yang merencanakan penggunaan penyedia jasa di luar negara Indonesia bahwa rencana tersebut tidak boleh merupakan upaya untuk menghindari/menghambat pengawasan atau pemeriksaan oleh Bank Indonesia. Sama halnya dengan penggunaan penyedia jasa TI domestik, penggunaan jasa TI pihak asing atau berlokasi di luar Indonesia harus melalui prosedur yang sama yaitu mulai dari *due diligence*, pemilihan penyedia jasa, pembuatan kontrak dan pengawasan, namun karena terkait dengan perbedaan yurisdiksi maka terdapat persyaratan lain yang harus diperhatikan oleh Bank. Bank yang akan menyelenggarakan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi di luar negeri harus mendapat persetujuan dari Bank Indonesia terlebih dahulu. Persetujuan tersebut termasuk untuk penyelenggaraan pada kantor Bank, kantor induk maupun kelompok usaha Bank di luar negeri. Sedangkan penggunaan pihak penyedia jasa di luar negeri untuk kegiatan TI lainnya seperti pengembangan program dan aplikasi yang digunakan Bank serta pemeliharaan *hardware & software* dapat mempergunakan pihak penyedia jasa di luar negeri tanpa harus terlebih dahulu mendapatkan persetujuan Bank Indonesia sepanjang tunduk kepada atau memenuhi ketentuan pada Pasal 18 PBI Penerapan Manajemen Risiko dalam Penggunaan TI dan ketentuan dalam pedoman ini.

Untuk memperoleh persetujuan Bank Indonesia selain persyaratan yang berlaku pada umumnya juga harus memenuhi hal-hal sebagai berikut:

- a. Bank harus melakukan analisis dan studi kelayakan terhadap kebijakan pemerintah, kondisi politik, sosial, ekonomi, dan hukum di negara dimana TI diselenggarakan. Selain itu perlu dilakukan pula analisis mengenai kemampuan Bank untuk

- memantau pihak penyedia jasa secara efektif, kemampuan Bank untuk melaksanakan *Business Continuity Plan* dan *early termination*;
- b. *country risk analysis* menunjukkan bahwa tidak terdapat dampak yang signifikan dari lokasi di luar negeri termasuk apabila terjadi sengketa dengan negara dimana pihak penyedia jasa berada;
 - c. Bank harus melakukan pengecekan apakah terdapat ketentuan di negara pihak penyedia jasa yang mengharuskan pihak penyedia jasa melakukan *information disclosure* atas data nasabah dalam hal atau kasus tertentu walaupun terdapat klausul kerahasiaan data nasabah di dalam kontrak perjanjian kerja;
 - d. pada prinsipnya Bank hanya dapat membuat perjanjian dengan pihak-pihak yang beroperasi di yurisdiksi yang secara umum mendukung klausula dan perjanjian kerahasiaan. Karena itu Bank harus memastikan bahwa perjanjian tertulis dengan penyedia jasa juga mencakup *choice of law* dan Bank memahami dampak dari hukum yang dipilih untuk menyelesaikan sengketa atau masalah hukum dikemudian hari;
 - e. untuk dapat memberikan setiap data yang diperlukan dalam rangka pengawasan oleh Bank Indonesia maka Bank harus memastikan bahwa struktur database dari setiap aplikasi yang digunakan dimiliki oleh Bank dan disimpan juga di kantor Bank di Indonesia dan terdapat petugas Bank di dalam negeri yang memahami struktur *database* termasuk *technical reference* dari *database* tersebut. Dengan demikian Bank harus meyakini bahwa penempatan *Data Center* di luar negeri tidak menghambat usaha-usaha untuk mengawasi dan merekonstruksi aktivitas Bank di dalam negeri (misalnya dari pembukuan, rekening, dan dokumen) secara tepat waktu setiap kali dibutuhkan;
 - f. Bank tidak boleh menempatkan *Data Center* di yurisdiksi dimana akses terhadap informasi oleh Bank Indonesia atau pihak-pihak yang ditunjuk oleh Bank Indonesia untuk bertindak atas nama Bank Indonesia terhadap *Data Center* dan *service provider*-nya dapat dihambat oleh batasan hukum atau administratif;
 - g. Bank harus melakukan kajian apakah penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi di luar negeri tersebut memungkinkan akses auditor intern Bank, ekstern maupun Bank Indonesia untuk memperoleh data dan informasi yang diperlukan dari penyelenggaraan TI secara tepat waktu setiap kali dibutuhkan;
 - h. Bank harus memberitahukan kepada Bank Indonesia bila ada otoritas di luar negeri yang meminta akses atas informasi mengenai nasabah Bank atau bila timbul situasi di mana hak akses yang dimiliki Bank atau Bank Indonesia untuk memperoleh informasi dan dokumen dibatasi atau ditolak;
 - i. apabila di kemudian hari dijumpai hambatan dalam pelaksanaan pemeriksaan penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis TI di luar negeri tersebut, Bank Indonesia dapat meminta perjanjian penggunaan jasa tersebut agar dihentikan;

- j. kajian yang dilakukan Bank mengenai *cost & benefit* harus menunjukkan bahwa manfaat bagi Bank melampaui biaya yang dibebankan oleh *provider/grup/parent* Bank termasuk peningkatan kualitas pelayanan kepada nasabah;
- k. kajian yang dilakukan Bank wajib mencakup pengembangan produk dan perencanaan sumber daya manusia. Diharapkan Bank mampu mengupayakan peningkatan kemampuan sumber daya manusia Bank baik di sisi penyelenggaraan TI yang digunakan maupun di sisi transaksi bisnis atau produk yang ditawarkan meskipun penyelenggaraan TI berlokasi di luar negeri;
- l. apabila Bank merupakan KCBA atau Bank yang dimiliki Lembaga Keuangan Asing maka Bank wajib menyampaikan hal-hal sebagai berikut dalam surat permohonan persetujuan:
 - 1) Surat Pernyataan dari otoritas pengawas lembaga keuangan di luar negeri bahwa pihak penyedia jasa TI merupakan cakupan pengawasan;
 - 2) Surat Pernyataan tidak keberatan dari otoritas pengawas setempat bila Bank Indonesia hendak melakukan pemeriksaan penyelenggaraan pusat data (*Data Center*) dan atau *Disaster Recovery Center* tersebut;
 - 3) Surat Pernyataan bahwa Bank secara berkala akan menyampaikan hasil penilaian yang dilakukan kantor Bank di luar negeri atas penerapan manajemen risiko pada pihak penyedia jasa. Surat Pernyataan ini mencantumkan periodisasi yang direncanakan;
 - 4) Hasil penilaian oleh kantor Bank di luar negeri atas penerapan manajemen risiko yang dilakukan oleh pihak penyedia jasa.
- m. khusus untuk rencana menyerahkan Pemrosesan Transaksi Berbasis TI (aktivitas atau kegiatan penambahan, penghapusan, perubahan dan otorisasi data yang dilakukan pada sistem aplikasi yang digunakan untuk memproses transaksi) kepada pihak lain di luar negeri, diperlukan kajian yang dapat membantu Bank memenuhi persyaratan tambahan lainnya lagi yaitu:
 - 1) memperhatikan aspek perlindungan kepada nasabah;
 - 2) aktivitas tidak merupakan atau terkait dengan *inherent banking functions* yaitu tabungan, giro, deposito maupun kredit (kecuali kartu kredit). Termasuk dalam hal ini aktifitas pembukaan rekening dan pemeliharaan master file data pribadi nasabah;
 - 3) dokumen pendukung administrasi keuangan atas transaksi yang dilakukan di kantor Bank di Indonesia dapat dipelihara di Indonesia;
 - 4) rencana bisnis yang menunjukkan adanya upaya untuk meningkatkan peran Bank bagi perekonomian di Indonesia.

Permohonan persetujuan wajib disampaikan paling lambat 4 (empat) bulan sebelum perubahan efektif dioperasikan sedangkan persetujuan atau penolakan akan diberikan Bank Indonesia paling lambat 3 (tiga) bulan setelah dokumen permohonan diterima secara lengkap. Selain persyaratan tersebut di atas, Bank Indonesia dapat

meminta tambahan persyaratan dari Bank dan atau melakukan pemeriksaan lebih lanjut. Permintaan kedua hal tersebut tergantung pada potensi dampak penggunaan pihak penyedia jasa TI terhadap Bank dan tingkat keyakinan atas dokumen yang disampaikan.

10.4. PROSES MANAJEMEN RISIKO

10.4.1. Penilaian Risiko

Penggunaan jasa pihak lain dalam menyelenggarakan TI Bank dapat memberikan kontribusi terhadap beberapa jenis risiko, yaitu:

- a. Risiko Operasional – ketidakmampuan penyedia jasa memenuhi kontrak;
- b. Risiko Hukum – ketidakpastian hukum atas perselisihan dengan pihak penyedia jasa dan/atau pihak ketiga dan atau tuntutan nasabah atas penyalahgunaan data nasabah oleh pihak penyedia jasa;
- c. Risiko Reputasi – ketidakpuasan nasabah karena ketidakmampuan penyedia jasa memenuhi SLA;
- d. Risiko Strategis – ketidakcocokan TI yang digunakan Bank dengan tujuan dan rencana strategis Bank yang dibuat untuk mencapai tujuan tersebut;
- e. Risiko Kepatuhan – ketidakmampuan Bank memenuhi ketentuan yang berlaku;
- f. *Country Risk* – kondisi di negara asing yang dapat mempengaruhi kemampuan penyedia jasa memenuhi standar pemberian jasa.

Dalam melakukan identifikasi, pengukuran dan pemantauan risiko Bank harus senantiasa mempertimbangkan ketiga faktor berikut ini:

- a. terkait dengan aktivitas dan fungsi yang diselenggarakan oleh pihak penyedia jasa meliputi sensitivitas data yang diakses, dilindungi atau dikendalikan oleh penyedia jasa, volume transaksi, dan tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis Bank;
- b. terkait dengan penyedia jasa seperti misalnya kondisi keuangan, kompetensi tenaga kerja, *turn over* manajemen dan tenaga kerja, pengalaman pihak penyedia jasa, profesionalitas;
- c. terkait dengan teknologi yang digunakan meliputi kehandalan (*reliability*), keamanan (*security*), ketersediaan (*availability*), dan ketepatan waktu (*timeliness*) serta kemampuan mengikuti perkembangan teknologi dan perubahan ketentuan.

10.4.2. Mitigasi Risiko

Berdasarkan PBI Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Bank tetap bertanggungjawab untuk setiap penerapan manajemen risiko Bank. Dengan demikian Bank wajib melakukan mitigasi risiko untuk setiap kelemahan dan/atau pelanggaran kebijakan dan prosedur pengamanan serta potensi risiko yang

dapat mengganggu kelangsungan penyelenggaraan TI yang digunakan oleh Bank, baik yang terjadi di Bank maupun di pihak penyedia jasa.

10.4.2.1. Business Continuity Plan (BCP)

Bank wajib memastikan bahwa risiko ketergantungan pada pihak penyedia jasa dapat dimitigasi sehingga Bank tetap mampu menjalankan bisnisnya apabila penyedia jasa wanprestasi, pemutusan hubungan atau dalam proses menuju likuidasi. Mitigasi risiko yang dapat dilakukan oleh Bank mencakup:

- a. memastikan bahwa pihak penyedia jasa memiliki BCP sesuai dengan jenis, cakupan dan kompleksitas aktivitas/jasa yang diberikan;
- b. secara aktif mendapatkan jaminan kesiapan BCP milik pihak penyedia jasa seperti pengujian secara berkala atas BCP;
- c. memiliki perjanjian penyimpanan *source code program (escrow agreement)* untuk aplikasi yang memiliki eksposur risiko tinggi, jika Bank tidak memiliki *source code* dari program aplikasi yang diselenggarakan oleh pihak penyedia jasa;
- d. dalam hal *source code* tidak dimiliki oleh penyedia jasa maka penyedia jasa harus memberikan jaminan kepada Bank, bahwa kelangsungan aplikasi didukung oleh *principal* pengembang *software*.

Untuk menjamin fungsi dan efektifitas BCP, Bank wajib menyusun dan melakukan pengujian BCP secara berkala, lengkap dan mencakup hal-hal yang signifikan yang didasarkan atas jenis, cakupan dan kompleksitas aktivitas atau kegiatan yang dilakukan oleh penyedia jasa. Disamping itu pihak penyedia jasa harus melakukan pengujian DRP di pihak penyedia jasa sendiri untuk sistem atau fasilitas TI maupun pemrosesan transaksi yang diselenggarakan tanpa melibatkan pihak Bank. Hasil pengujian DRP pihak penyedia jasa tersebut digunakan Bank untuk mengkinikan DRP ataupun BCP yang dimiliki Bank.

10.4.2.2. Pengendalian Risiko Lainnya

Meskipun Bank maupun pihak penyedia jasa sudah menggunakan sistem yang canggih namun masih memungkinkan adanya penyimpangan dari dalam seperti misalnya kesalahan manusia, penerapan prosedur yang lemah serta pencurian pegawai (*employee theft*). Bank harus memastikan adanya pengendalian pengamanan dasar untuk memitigasi risiko yang mencakup hal-hal sebagai berikut:

- a. pihak penyedia jasa harus melakukan penelitian latar belakang para pegawainya karena serangan dari dalam lebih susah dicegah;
- b. menutup kemungkinan *orphan accounts* digunakan untuk transaksi. *Password & e-mail* dari pegawai yang telah keluar harus segera dihapus;
- c. lingkungan fisik baik di pihak penyedia jasa maupun di Bank harus selalu dipastikan aman, seperti pemantauan orang yang keluar masuk ruangan, kemungkinan bencana banjir dan kebakaran;

- d. lingkungan elektronik baik di pihak penyedia jasa maupun di Bank harus selalu dipastikan aman;
- e. prosedur pengamanan dikinikan secara berkala agar selalu mematuhi ketentuan yang berlaku dan sesuai *best practices*;
- f. buat kelompok yang melakukan *intrusion-detection* secara berkala baik didalam Bank maupun menyewa para profesional. Lakukan pemantauan kemajuannya dan pastikan standar diterapkan secara memadai;
- g. pastikan kewajiban pihak penyedia jasa untuk melakukan pengendalian keamanan terhadap seluruh fasilitas teknologi informasi yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian;
- h. pastikan agar sebelum perjanjian ditandatangani pihak penyedia jasa memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan Bank untuk masing-masing jenis data berdasarkan sensitifitas kerahasiaan data;
- i. usahakan agar biaya yang dikeluarkan untuk pengamanan masing-masing sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko yang telah ditetapkan oleh Bank.

10.5. PENGENDALIAN INTERN DAN AUDIT INTERN

10.5.1. Pemantauan/Pengawasan

Bank wajib memiliki program pemantauan untuk memastikan penyedia jasa telah melaksanakan pekerjaan/memberikan jasa sesuai dengan kontrak. Sumber daya untuk mendukung program ini dapat bervariasi tergantung pada kritikalitas dan kompleksitas sistem, proses dan jasa yang dikerjakan pihak lain.

Bank wajib melakukan *pre* dan *post-review* penyedia jasa pihak lain untuk memastikan bahwa kebijakan dan prosedur manajemen risiko Bank telah dilakukan secara efektif.

Selanjutnya, *review performance* dan pencapaian *Service Level Agreement (SLA)* dilakukan secara berkala yang didokumentasikan dalam bentuk laporan. Pemantauan wajib dilakukan terhadap laporan tahunan hasil pemeriksaan penyedia jasa.

10.5.2. Audit Intern

Bank wajib melaksanakan fungsi audit terhadap pihak penyedia jasa, baik dilakukan oleh audit intern Bank maupun pihak audit ekstern yang ditunjuk oleh Bank. Apabila pihak penyedia jasa memberikan layanan kepada lebih dari satu Bank maka pihak penyedia jasa dapat menunjuk auditor TI independen untuk melakukan audit atas layanan yang diberikan kepada masing-masing Bank. Hasil pemeriksaan yang dilakukan oleh auditor TI yang independen ini untuk kepentingan masing-masing Bank sehingga SKAI Bank tetap bertanggung jawab atas hasil audit tersebut dan wajib memastikan kesesuaian pelaksanaan audit dengan kebijakan dan prosedur audit Bank.

Ruang lingkup audit sesuai dengan cakupan pekerjaan/jasa sebagaimana yang tertuang dalam kontrak perjanjian. Area yang diaudit antara lain seperti *IT Systems, data security, internal control frameworks* dan *business contingency plan*.

Bank wajib memastikan bahwa, Bank Indonesia atau pihak lain yang ditugaskan oleh Bank Indonesia memiliki hak akses ke penyedia jasa dan Bank untuk mendapatkan catatan-catatan dan dokumen transaksi, serta informasi Bank yang disimpan atau diproses oleh penyedia jasa serta hak akses terhadap laporan dan temuan audit terhadap penyedia jasa yang terkait dengan jasa yang diberikan kepada Bank.

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:

jalan masuk. Suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat *hardware* atau *software* tertentu, seperti modem yang digunakan untuk membuka akses internet. Perangkat *hardware* atau *software* 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 di komputer yang menyimpan informasi mengenai kegiatan administrator

5. AES (Advanced Encryption Standard):

standar enkripsi berdasarkan algoritma *block cipher* dengan panjang blok tertentu (128 bit) dan panjang kunci yang bervariasi (AES-128, AES-192, AES-256). AES dianggap sebagai pengganti DES.

6. Agile Software Development:

merupakan kerangka teknis pengembangan system yang mengutamakan pengembangan secara iterasi/ berulang-ulang dalam siklus (SDLC) suatu proyek. Tahapan yang harus dilalui dalam setiap iterasi merupakan bagian dari SDLC, seperti perencanaan, analisis kebutuhan, desain, pengembangan, uji coba dan dokumentasi.

7. Arm's Length Principle:

suatu prinsip kerjasama yang wajar dan saling menguntungkan dimana masing-masing pihak yang akan membuat perjanjian kerjasama memiliki daya tawar (*bargaining power*) yang sama walaupun pihak penyedia jasa merupakan pihak terkait.

8. Automated Teller Machine (ATM):

suatu terminal/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.

9. Audit Trail:

file di komputer yang menyimpan informasi mengenai kegiatan *user* atau komputer yang tersimpan secara kronologis, yang dapat digunakan untuk audit atau penelusuran.

10. Authentication:

kemampuan dari setiap pihak dalam transaksi untuk menguji kebenaran dari pihak lainnya.

11. 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.

12. Backup:

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 *Data Center* dan atau *off site* di lokasi alternatif.

13. Backup Site:

lokasi penyimpanan *backup* komputer dan file yang terpisah dengan *Data Center*.

12. Backlog project:

adanya proyek pengembangan sistem aplikasi yang tertunda pelaksanaannya.

13. Business Continuity Management (BCM):

proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional Bank tetap dapat berfungsi walaupun terdapat gangguan/bencana guna melindungi kepentingan para *stakeholder*.

14. Business Continuity Plan (BCP):

suatu dokumen tertulis yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan/bencana dan proses pemulihan agar kegiatan operasional Bank dan pelayanan kepada nasabah tetap dapat berjalan. Rencana tindak tertulis tersebut melibatkan seluruh sumber daya Teknologi Informasi (TI) termasuk sumber daya manusia yang mendukung fungsi bisnis dan kegiatan operasional yang kritikal bagi Bank.

15. Business Impact Analysis (BIA):

Proses untuk memastikan akibat yang ditimbulkan dari ketidakterseediaannya dukungan semua resource. Pada fase ini mencakup identifikasi beragam kejadian yang dapat mengakibatkan kelangsungan kegiatan operasional dan financial, sumber daya manusia dan dampak terhadap reputasi perusahaan. BIA merupakan langkah kritikal dalam pengembangan BCP.

16. Business Recovery Center/Crisis Center/Business Resumption Center:

Lokasi yang digunakan sebagai pusat kegiatan bisnis pada saat proses *recovery* setelah terjadinya *disaster*.

17. Client Server:

Arsitektur komputer dimana terdapat 2 jenis titik pertemuan berupa *client* dan *server*. Tiap *client* dapat mengirim permintaan data ke satu atau lebih server yang saling terhubung. *Server* selanjutnya menerima, memproses dan menjawab permintaan data tersebut.

18. Cold Sites:

lokasi alternatif (DRC) yang hanya memiliki fasilitas yang sifatnya sangat mendasar (seperti: listrik, AC dan ruangan) dan belum memiliki konfigurasi komputer yang kompatibel serta belum terdapat *backed up data* lengkap sebagaimana di *hot sites DRC*. Lokasi ini siap untuk menerima penggantian perangkat komputer yang dibutuhkan pada saat *user* harus pindah dari *Data Center* ke lokasi alternatif. Untuk itu apabila lokasi ini akan digunakan diperlukan tambahan waktu sebelum siap digunakan untuk menggantikan *Data Center* saat terjadi *disaster*.

17. Communicative E-Banking:

pelayanan jasa Bank kepada nasabah melalui media elektronik dalam bentuk komunikasi atau melakukan interaksi dengan Bank penyedia layanan secara terbatas dan tidak terdapat eksekusi transaksi.

18. Contingency Plan:

Prosedur yang berisikan mengenai rencana atau langkah-langkah secara manual yang harus dilakukan oleh unit bisnis untuk menjalankan kegiatan operasional bisnis pada saat proses *recovery* sedang dilakukan.

19. Controller (Host-Front End):

telecommunication control unit adalah sejenis komputer mini yang berfungsi untuk mengontrol kinerja perangkat keras dan perangkat lunak yang ada pada suatu sistem seperti terminal komputer / ATM, jaringan komunikasi atau sarana komputer lainnya.

20. Cost and Benefit Analysis:

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 *outsourcing* atau pemilihan penyedia jasa.

21. Cybersquatting:

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.

22. Database:

basis data yaitu representasi kumpulan fakta yang saling berhubungan disimpan secara bersama sedemikian rupa dan tanpa pengulangan (redundansi) yang tidak perlu, untuk memenuhi berbagai kebutuhan. Data perlu disimpan dalam basis data untuk keperluan penyediaan informasi lebih lanjut. Data di dalam basis data perlu diorganisasikan sedemikian rupa, supaya informasi yang dihasilkan berkualitas. Organisasi basis data yang baik juga berguna untuk efisiensi kapasitas penyimpanannya. Dalam maksud yang sama, bisa juga diartikan sebagai sekumpulan informasi yang disusun sedemikian rupa untuk dapat diakses oleh sebuah *software* tertentu. *Database* tersusun atas bagian yang disebut *field* dan *record* yang tersimpan dalam sebuah *file*. Sebuah *field* merupakan kesatuan terkecil dari informasi dalam sebuah *database*. Sekumpulan *field* yang saling berkaitan akan membentuk *record*.

23. Data Center:

fasilitas utama pemrosesan data Bank yang terdiri dari perangkat keras dan perangkat lunak untuk mendukung kegiatan operasional Bank secara berkesinambungan.

24. Defacing:

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

25. DES (Data Encryption Standar):

standar enkripsi berdasarkan algoritma *block cipher*. Standar ini telah lama digunakan dan sering dianggap tidak dapat lagi memberikan pengamanan yang memadai.

26. Denial of Service Attack:

serangan terhadap sistem teknologi informasi 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.

27. 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" (CA) seperti VeriSign (www.verisign.com) and Thawte (www.thawte.com).

28. Digital signatures:

suatu informasi berupa tanda-tanda tertentu yang berbetuk *digital* yang dapat memastikan otentikasi pengirim, integritas data, dan tak dapat disangkal.

29. Disaster Recovery Plan (DRP):

dokumen yang berisikan rencana dan langkah-langkah mendapatkan kembali akses data, *hardware* dan *software* yang diperlukan agar Bank dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya *disaster*. DRP menekankan pada aspek teknologi.

30. Disaster Recovery Center (DRC):

suatu lokasi alternatif yang dapat digunakan pada saat Pusat Data (*Data Center*) mengalami gangguan atau tidak dapat berfungsi akibat adanya *disaster* antara lain karena tidak adanya aliran listrik ke ruang komputer, kebakaran, ledakan atau kerusakan pada komputer, yang digunakan sementara waktu selama dilakukannya pemulihan Pusat Data (*Data Center*) Bank untuk menjaga kelangsungan kegiatan usaha (*business continuity*).

31. Disposal Media Backup:

proses penghancuran terhadap media *backup* yang sudah melewati masa retensi dan tidak digunakan

32. Down Time:

Lamanya sistem tidak dapat berfungsi dan digunakan oleh pengguna karena adanya gangguan *hardware*, *software* dan komunikasi.

33. Due Diligence:

suatu proses untuk mendapatkan informasi selengkap-lengkapny mengenai penyedia jasa untuk menilai reputasi, kemampuan operasional, manajerial, kondisi keuangan, strategi pengembangan di masa mendatang dan kemampuan mengikuti perkembangan teknologi terkini.

34. E-money atau stored value atau prepaid card:

produk yang merupakan media yang dipakai dalam mekanisme sistem pembayaran melalui pembayaran di *point of sales (merchant)*, transfer antar dua media elektronik atau jaringan komputer menggunakan nilai uang yang tersimpan pada kartu atau produk tersebut.

35. Electronic Data Capture/Point of Sales Terminal:

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.

36. Electronic Fund Transfer:

transfer dana antar rekening melalui sistem pembayaran yang menggunakan media elektronik. EFT dapat dilakukan pada transaksi keuangan melalui telepon, terminal komputer, dll.

37. Enkripsi:

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

38. Escrow Agreement:

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

39. Exception Handling:

mekanisme untuk menangani munculnya kondisi yang tidak diharapkan yang dapat mengubah alur normal suatu sistem aplikasi.

40. Firewall:

peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan seleksi atas lalu lintas data/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 mengkompromikan komputer internal yang dapat menyebabkan *data corruption* dan atau *denial of service* bagi pengguna yang diotorisasikan.

41. Full System Back up:

system backup yang mencakup keseluruhan sistem yang digunakan.

42. 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.

43. Hardcopy:

salinan data/informasi komputer dalam bentuk tercetak atau dikenal dengan *printout*.

44. Hardening:

merupakan proses/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*, *firewall*.

45. Hash Function:

suatu cara untuk mengubah data (biasanya berbentuk pesan atau file) menjadi suatu angka tertentu yang dapat digunakan oleh komputer untuk menghasilkan data asalnya kembali

46. Hot Card File:

file yang menyimpan informasi mengenai kartu magnetis yang harus ditelan oleh mesin seperti ATM, karena kartu tersebut tidak memenuhi syarat untuk dapat dioperasikan.

47. Hot Sites:

Lokasi alternatif (DRC) yang memiliki konfigurasi komputer yang secara penuh (*hardware, network, system software* dan aplikasi) dan kompatibel dengan *Data Center*. Pada umumnya dapat dioperasikan segera setelah terjadinya *disaster, sehingga data* secara kontinu di *backup* menggunakan koneksi *live* antara *Data Center* dan DRC.

48. Hub:

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

49. Informational E-Banking:

pelayanan jasa Bank kepada nasabah melalui media elektronik baik internet, *mobile phone*, telepon, dll. dan tidak terdapat eksekusi transaksi.

50. Interoperabilit:

- 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).

51. Interface / Integration Testing:

uji coba oleh quality assurance dan pengguna akhir untuk menguji antar muka / *interface* komponen perangkat lunak yang terintegrasi, termasuk keterhubungannya dengan sistem lain.

52. IT Control:

pengendalian Teknologi Informasi (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 mencakup pengendalian di manajemen dan organisasi TI Bank, pengendalian akses baik logik maupun fisik, pelaksanaan DRP/BCP, dll. Pengendalian aplikasi diperlukan untuk memastikan kelengkapan dan keakuratan dalam setiap tahap pemrosesan informasi. Pengendalian aplikasi diintegrasikan dengan sistem aplikasi yang digunakan untuk pemrosesan transaksi.

53. Keylogger:

ancaman berupa perangkat lunak atau perangkat hardware yang digunakan untuk memperoleh informasi (PIN, password) yang diketikkan pengguna pada *keyboard* (biasanya di warung internet).

54. Library:

kumpulan perangkat lunak atau data yang memiliki fungsi tertentu dan disimpan serta siap untuk digunakan.

55. Logic Bomb:

suatu kode yang sengaja dimasukkan di dalam suatu sistem perangkat lunak yang pada suatu kondisi tertentu akan melakukan serangkaian fungsi yang bersifat merusak.

56. Man-in-the-middle-attack:

jenis serangan terhadap sistem teknologi informasi dimana hacker/penyerang menyadap pesan yang dikirimkan pengirim kepada penerima dan/atau selanjutnya mengubah isi pesan dan mengirimkannya kembali kepada penerima. Hacker/penyerang akan menggunakan program yang tampak seperti *server* bagi *client* dan tampak sebagai *client* bagi *server*.

57. Maximum Tolerable Outage / Recovery Time Objective:

Lamanya waktu yang dapat ditolerir pada saat sistem tidak dapat berfungsi akibat adanya gangguan. RTO mengindikasikan waktu tercepat/terpendek (*earliest point in time*) yang diperlukan agar kegiatan bisnis operasional dapat kembali berjalan setelah adanya gangguan (*disaster*).

58. Mobile Banking:

Layanan yang memungkinkan nasabah Bank melakukan transaksi perbankan melalui *handphone*. *Mobile banking* umumnya dilakukan melalui sms atau *mobile internet* namun dapat juga menggunakan program khusus yang di-*download* melalui *handphone*.

59. Modem (Modulator Demodulator):

alat yang ditempatkan diantara mesin komunikasi dan saluran telepon untuk memungkinkan transmisi pulsa digital. Saluran telepon hanya dapat menyalurkan sinyal dalam bentuk suara/analog dan tidak dapat membawa sinyal digital seperti yang dihasilkan oleh peralatan komputer. Modulator akan mengubah pulsa bit menjadi nada dan mengirimkannya melalui jaringan komunikasi, sedangkan demodulator akan mengubahnya menjadi bit yang sesuai.

60. Network interface:

titik interkoneksi antara terminal pengguna, mesin, atau suatu jaringan dengan jaringan lain.

61. Non-repudiation:

suatu cara untuk memastikan kebenaran pengirim dan penerima sehingga tidak ada pihak yang dapat menyangkal.

62. Off-line:

sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

63. Off the shelf:

tersedia apa adanya, dibuat bukan berdasarkan pesanan khusus.

64. Orphan Account:

rekening yang dimiliki pengguna yang telah keluar dari suatu organisasi.

65. Outsourcing:

pengguna pihak lain (eksternal) dalam penyelenggaraan teknologi informasi Bank yang menyebabkan Bank memiliki ketergantungan terhadap jasa yang diberikan pihak lain tersebut secara berkesinambungan dan atau dalam periode tertentu.

66. Parallel Distributed Computing:

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.

67. Password:

kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan.

68. 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.

69. Patch Management:

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

70. Pengamanan Fisik:

suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap area komputerisasi serta peralatan/fasilitas pendukung.

71. Pengamanan Logik:

suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap sistem komputer dan informasi yang tersimpan di dalamnya yang meliputi penggunaan *user ID*, *password*, dll.

72. Personal Identification Number (PIN):

rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi pengguna komputer, pengguna ATM, *internet banking*, *mobile banking*, dll.

73. Perusahaan *Switching*:

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

74. *Phising*:

salah satu bentuk teknik *social engineering* untuk memperoleh informasi rahasia seseorang secara ilegal. *Phising* dapat dalam bentuk *e-mail* palsu yang seolah-olah berasal dari Bank, perusahaan kartu kredit, dll untuk memperoleh informasi seperti PIN, Password, dll.

75. *Phone Banking*:

layanan yang memungkinkan nasabah Bank melakukan transaksi perbankan melalui telepon.

76. *Piggybacking*:

- (i) tindakan di mana seseorang memasuki ruangan dengan mengikuti orang lain yang memiliki akses ke ruangan tersebut;
- (ii) suatu cara untuk menyusup atau mengubah transmisi dengan melekat pada jaringan telekomunikasi yang terotorisasi.

77. *Pita magnetis*:

suatu pita perekam yang digunakan untuk media penyimpan data. Setiap karakter ditulis melintasi lebar pita dalam bentuk titik-titik yang diberi muatan magnet, Pembacaan dari dan penulisan ke pita dilakukan dengan menggerakkan permukaan pita melintasi suatu *read/write head* sebuah *tape drive*.

78. *Platform*:

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

79. *Point of Sales*:

perangkat keras atau terminal komputer berupa *cash register* atau terminal *debit/credit verification* yang dapat menerima informasi penjualan eceran di tempat penjualan dan memasukkan data sebagai input ke komputer.

80. *Power User*:

user id yang memiliki kewenangan sangat luas.

81. *Process Control*:

kontrol yang dimiliki oleh penyedia jasa terutama terkait dengan proses jasa yang diberikan kepada Bank untuk menjamin kualitas jasa dari sisi kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).

82. Public Key Infrastructure:

suatu pengolahan/pengaturan dimana suatu pihak ketiga yang dapat dipercaya menyediakan pemeriksaan secara seksama dan memastikan keabsahan suatu identitas.

83. Rapid Application Development (RAD):

metodologi pengembangan sistem yang terdiri atas pengembangan secara iterasi dan pengembangan prototipe (*prototyping*) yang dipercepat sehingga manfaat, fitur dan kecepatan eksekusi program tidak optimal.

84. 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*.

85. Restore:

mengembalikan pada fungsi atau kondisi semula sebelum terjadi *disaster*.

86. Restricted area:

Area yang hanya dapat dimasuki oleh orang yang telah mendapatkan hak akses.

87. Router:

peralatan jaringan yang meneruskan suatu paket data/informasi dan memilih rute terbaik untuk ditempuh untuk menyampaikan data/informasi tersebut.

88. Service Level Agreement:

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.

89. Social Engineering:

teknik pembohongan melalui perilaku sosial yang dilakukan oleh *hacker* untuk mengelabui orang agar memberikan informasi rahasia seperti PIN, *Password*, dll.

90. Softcopy:

salinan data atau dokumen dalam bentuk file elektronik.

91. Software Patch:

program yang dibuat oleh vendor untuk meningkatkan kinerja dan meningkatkan keamanan dari produk perangkat lunaknya, baik perangkat lunak yang berupa sistem operasi, *database*, *tools* pengembangan aplikasi dll.

92. Source Code:

instruksi program perangkat lunak yang ditulis dalam suatu format (bahasa) dan dapat dibaca oleh manusia.

93. 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.

94. Spyware:

perangkat lunak yang mengumpulkan informasi-informasi sensitif tentang pengguna tanpa sepengetahuan atau ijin dari pengguna.

95. Stress Testing:

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

96. Subcontractor:

penyedia jasa lain yang digunakan oleh penyedia jasa yang dikontrak oleh Bank.

97. Switch:

peralatan dalam jaringan yang meneruskan paket informasi kepada *address* atau peralatan yang dituju.

98. System:

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

99. System Development Life Cycle:

siklus pengembangan sistem yang meliputi langkah-langkah sebagai berikut: (1) *system planning*, (2) *system analysis*, (3) *system design*, (4) *system selection*, (5) *system implementation*, (6) *system maintenance*.

100. System Source:

salah satu informasi yang diperlukan dalam inventarisasi media penyimpan yaitu keterangan dari sistem mana suatu data diperoleh.

101. System Testing:

uji coba yang dilakukan *quality assurance* untuk menguji fungsionalitas keseluruhan system aplikasi, termasuk tiap objek yang terdapat dalam system aplikasi tersebut.

102. System Log:

file di komputer yang menyimpan informasi mengenai kegiatan sistem atau komputer.

103. Technical Reference:

pedoman teknis dari aplikasi database yang antara lain berisi penjelasan mengenai struktur database yang terdiri dari tables dan fields termasuk relasi antar tabel berupa *entiry relationship diagram (ERD)*.

104. Transactional E-Banking:

pelayanan jasa Bank kepada nasabah melalui media elektronik dimana terdapat eksekusi transaksi.

105. 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”.

106. UnitTesting:

uji coba yang dilakukan oleh pengembang untuk menguji fungsionalitas dari modul-modul kecil dalam program perangkat lunak.

107. Upload dan Dowload:

transfer data elektronik antara dua komputer atau sistem yang sejenis.

108. User Acceptance Test:

ujicoba akhir oleh pengguna untuk menguji keseluruhan fungsionalitas dan *interoperability* dari suatu system aplikasi.

109. User Log:

file di komputer yang menyimpan informasi mengenai kegiatan user seperti waktu login dan *log-out*

110. 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 e-mail, game, program bajakan* dll.

111. War Driving:

suatu tindakan untuk mendapatkan jaringan wi-fi (*wireless local area network*) dengan menggunakan perangkat yang dapat mendeteksi adanya jaringan wi-fi, seperti laptop atau PDA.

112. Warm Sites:

Lokasi alternatif (DRC) yang memiliki sebagian konfigurasi dari *Data Center* dan pada umumnya hanya terdiri dari koneksi jaringan dan beberapa perangkat pendukung tanpa adanya *main computer* (komputer utama). Sistem tidak otomatis berpindah tetapi masih terdapat proses manual meskipun dilakukan seminimal mungkin.

113. Web Site:

web page 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.

114. Worm:

program komputer yang dirancang untuk memperbanyak diri secara otomatis dengan melekat pada *e-mail* atau sebagai bagian dari pesan jaringan. *Worm* menyerang jaringan dan berakibat kepada penuhnya *bandwith* yang terpakai sehingga menghambat laju pengiriman data pada jaringan.

Lampiran 1.1**CONTOH PENILAIAN RISIKO**

Seperti telah dijelaskan dalam Bab I Manajemen Bank perlu memiliki dokumentasi risiko agar risiko yang diidentifikasi dan dinilai atau diukur dapat dipantau oleh manajemen yang biasa disebut dengan *Risk Register*. Untuk menghasilkan risk register ini perlu langkah-langkah tertentu yang harus dilakukan. Saat ini terdapat berbagai macam pendekatan, langkah dan metode dapat digunakan dalam penilaian risiko penggunaan Teknologi Informasi (TI) misalnya dengan pendekatan aset atau pendekatan proses. Bank dapat menentukan sendiri pendekatan, langkah dan metode yang akan dilakukan. Berikut ini adalah contoh **penilaian risiko pengamanan informasi** yang menggunakan **pendekatan aset**.

1. Dokumen hasil Identifikasi dan Pengukuran Risiko (*Risk Register*)

No	Aset	Deskripsi Risiko	Analisa Kerawanan	Inheren			Pengendalian yg Ada	Residual			Nilai Risiko Akhir Diharapkan
				Kecenderungan	Dampak	Nilai Risiko Dasar		Kecenderungan	Dampak	Nilai Risiko Akhir	
0	1	2	3	4	5	6	7	8	9	10	11

2. Identifikasi Risiko**2.1. Identifikasi (penentuan klasifikasi) Aset**

Kolom No.1 yaitu aset, diisi dengan nama atau jenis aset yang dihasilkan dalam menjalankan proses bisnis bank dan aset yang mendukung terlaksananya proses bisnis tersebut. Aset yang dimaksud bukan aset secara akuntansi, namun segala sesuatu yang mempunyai nilai bagi organisasi dan harus diamankan termasuk data, perangkat lunak, perangkat keras, jaringan komunikasi dan data, sarana pendukung dan sumber daya manusia. Tentukan pemilik aset tersebut dan identifikasi tingkatan penting tidaknya (kritikal) aset tersebut bagi unit kerja pengguna dan unit kerja penyelenggara TI. Untuk proses identifikasi ini Bank menetapkan terlebih dahulu kriteria penilaian tertentu yang akan digunakan misalnya seperti yang terdapat pada contoh di tabel berikut:

Aspek	Analisa Sensitivitas	Kriteria Penilaian		
		<i>High</i>	<i>Medium</i>	<i>Low</i>
<i>Confidentiality</i>	Berapa besar kerugian yang ditimbulkan apabila terjadi hilangnya kerahasiaan atas suatu informasi?	Jika kerugian yang ditimbulkan sangat signifikan karena informasi yang bocor sangat sensitif atau hanya bisa diakses oleh personil tertentu yang telah diberi otorisasi.	Jika kerugian yang ditimbulkan tidak signifikan karena informasi tidak sensitif atau akses informasi oleh berbagai pihak di organisasi.	Jika kerugian yang ditimbulkan sangat kecil karena informasi bersifat umum atau dapat diakses oleh siapa saja.
<i>Integrity</i>	Berapa besar dampak/kerugian terhadap jalannya proses bisnis apabila suatu aset tidak digunakan dengan benar, tidak lengkap, tidak akurat dan tidak dikinikan?	Jika dampak yang ditimbulkan sangat signifikan seperti mengakibatkan tidak berjalannya proses bisnis dan menimbulkan potensi dilakukannya penyimpangan yang mengarah pada nilai uang yang cukup signifikan.	Jika dampak yang ditimbulkan tidak signifikan seperti mengakibatkan tidak berjalannya proses bisnis yang tidak signifikan, kesalahan dalam pengambilan keputusan.	Jika dampak yang ditimbulkan sangat kecil dan tidak mengganggu proses bisnis.
<i>Availability</i>	Berapa besar dampak/kerugian yang ditimbulkan apabila terjadi ketidaktersediaan suatu aset?	Jika dampak yang ditimbulkan sangat signifikan seperti mengakibatkan tidak berjalannya proses bisnis.	Jika dampak yang ditimbulkan tidak signifikan karena aset dapat digantikan dengan biaya atau waktu yang memadai sehingga hanya mengakibatkan penurunan efisiensi dan efektivitas atas jalannya proses bisnis.	Jika dampak yang ditimbulkan sangat kecil karena proses bisnis tetap berjalan tanpa aset tersebut atau aset bisa diganti dengan cepat.

Aset yang telah diklasifikasikan sesuai analisa sensitivitas dan penentuan tingkat kritikal seperti dalam tabel diatas kemudian dicantumkan pada kolom 1 di form *Risk Register*.

Contoh : Informasi nasabah dalam bentuk *hardcopy*.

2.2. Identifikasi risiko dan evaluasi risiko yang terkait dengan aset

Kolom 2 di *Risk Register* diisi dengan hasil identifikasi dan evaluasi pengguna dan penyelenggara TI terhadap potensial kegagalan atau kelemahan proses pengamanan yang ada/diterapkan Bank atas aset yang telah didefinisikan, sehingga berpengaruh secara signifikan terhadap kinerja Bank. Satu aset dapat memiliki beberapa risiko. Contoh pencantuman di Kolom 2 (Deskripsi Risiko): Informasi bocor kepada pihak yang tidak berwenang.

2.3. Analisa Kerawanan

Kolom 3 *Risk Register* diisi dengan faktor yang rawan dapat menyebabkan terjadinya kegagalan atau kelemahan pengamanan TI (risiko) yang telah diidentifikasi pada kolom 2. Tiap risiko dapat memiliki beberapa kerawanan.

Contoh pencantuman di kolom 3:

- Pengamanan terhadap lemari penyimpanan arsip kurang memadai;
- Informasi nasabah tidak disimpan dengan baik pada tempat yang seharusnya.

3. Pengukuran Risiko

Besarnya pengaruh risiko dapat diketahui dengan menilai kecenderungan risiko dan dampak yang dapat ditimbulkan oleh risiko tersebut terhadap proses bisnis. Kriteria pengukuran yang digunakan mengacu kepada metode *risk assessment* yang berlaku di Bank. Proses ini dilakukan oleh personil yang mengetahui proses bisnis dan pengamanan atas informasi di proses tersebut. Kolom 4, 5, dan 6 diisi dengan hasil pengukuran Bank atas kecenderungan dan dampak dari risiko **sebelum** pengendalian dilakukan terhadap aset berisiko tersebut. Sedangkan kolom 8, 9 dan 10 diisi dengan hasil pengukuran Bank atas kecenderungan dan dampak dari risiko **setelah** pengendalian dilakukan terhadap aset berisiko tersebut.

3.1. Pengukuran Kecenderungan (*Probability*)

Kolom 4 *Risk Register* diisi dengan Kecenderungan **Inheren** yang merupakan kemungkinan terjadinya risiko sebelum adanya pengendalian. Kolom 8 diisi dengan Kecenderungan **Residual** yang merupakan kemungkinan terjadinya risiko setelah adanya pengendalian. Kecenderungan dapat diukur dengan suatu kriteria pengukuran, yaitu nilai kuantitatif dari kecenderungan terjadinya risiko yang disebutkan pada deskripsi risiko. Kuantifikasi kecenderungan dapat

berupa ukuran terjadinya risiko dalam satuan waktu seperti frekuensi kejadian setiap hari, setiap minggu, setiap bulan, atau setiap tahun.

Contoh kriteria pengukuran kecenderungan:

Level	Frekuensi Kejadian	Potensi Terjadi
5	Sangat sering terjadi	Potensi terjadi tinggi dalam jangka pendek
4	Lebih sering terjadi	Potensi terjadi tinggi dalam jangka panjang
3	Cukup sering terjadi	Potensi terjadi sedang
2	Jarang terjadi	Potensi terjadi kecil
1	Hampir tidak pernah terjadi	Kemungkinan terjadi sangat kecil

Contoh pencantuman hasil pengukuran Kecenderungan Inheren pada kolom 4 di form *Risk Register* : **Level 4**

Contoh pencantuman hasil pengukuran Kecenderungan Residual pada kolom 8 di form *Risk Register* : **Level 3**

3.2. Pengukuran Dampak (*impact/severity*)

Kolom 5 *Risk Register* diisi dengan Dampak **Inheren** yang menggambarkan tingkatan kerusakan yang disebabkan oleh terjadinya risiko relatif terhadap aset **sebelum** ada/diterapkannya pengendalian. Kolom 9 diisi dengan Dampak **Residual** yang menggambarkan tingkatan kerusakan yang disebabkan oleh terjadinya risiko relatif terhadap aset **setelah** ada/diterapkannya pengendalian.

Contoh klasifikasi dampak :

Nilai	Potensi gangguan terhadap Proses Bisnis	Potensi penurunan Reputasi
5	Aset Pemrosesan Informasi mengalami kegagalan total sehingga keseluruhan bisnis bank tidak tercapai.	Kerusakan reputasi yang mengakibatkan penurunan reputasi yang serius dan berkelanjutan dimata nasabah/stakeholders utama, pasar uang dan masyarakat secara global dan regional.
4	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan aktivitas bisnis bank mengalami penundaan sampai Aset	Kerusakan reputasi yang tidak menyeluruh – hanya nasabah atau partner bisnis (<i>counterparties</i>) tertentu.

Nilai	Potensi gangguan terhadap Proses Bisnis	Potensi penurunan Reputasi
	Pemrosesan Informasi yang terkait pulih	
3	Aset Pemrosesan Informasi mengalami gangguan yang menyebabkan sebagian bisnis bank mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih	Kerusakan reputasi yang tidak menyeluruh – hanya di divisi/bagian/tim tertentu.
2	Aset Pemrosesan Informasi mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya.	Kerusakan reputasi yang tidak menyeluruh - hanya satuan kerja tertentu.
1	Tidak menyebabkan gangguan terhadap operasional proses bisnis	Tidak berpengaruh pada reputasi.

Contoh pencantuman hasil pengukuran dampak pada kolom 5 di form *Risk Register* : **Level 5**

Contoh pencantuman hasil pengukuran dampak pada kolom 8 di form *Risk Register* : **Level 2**

3.3. Penentuan Nilai Risiko

Kolom 6 *Risk Register* diisi dengan **Nilai Risiko Dasar (NRD)** yaitu tingkatan risiko aset **sebelum** ada/diterapkannya pengendalian. Kolom 10 *Risk Register* diisi dengan **Nilai Risiko Akhir (NRA)** yaitu tingkatan risiko aset **setelah** ada/diterapkannya pengendalian. Seperti telah dijelaskan dalam Bab I, Bank dapat menentukan sendiri metode pemeringkatan dalam matriks pengukuran risiko. Penilaian risiko pada contoh ini diukur menggunakan 3 tingkatan yang meliputi : *Low*, *Medium*, dan *High* sebagai berikut:

Kecenderungan	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Low	Medium	High	High
	2	Low	Low	Medium	Medium	High
	1	Low	Low	Medium	Medium	High
		1	2	3	4	5

Dampak

Contoh pencantuman hasil penentuan NRD di kolom 6: **High**

Contoh pencantuman hasil penentuan NRA di kolom 10: **Medium**

4. Identifikasi Pengendalian yang Diimplementasikan

Kolom 7 *Risk Register* diisi dengan langkah-langkah pengendalian yang telah diimplementasikan oleh Bank untuk mengurangi risiko atas aset yang diidentifikasi seperti:

- kebijakan dan prosedur Bank terkait aset;
- penggunaan teknologi tertentu untuk mengendalikan risiko secara otomatis atau tersistem seperti *audit log, on line approval, parameter value* di sistem.

Contoh pencantuman kontrol di kolom 7 untuk aset yang berupa Informasi nasabah dalam bentuk *hardcopy*:

- ketentuan mengenai pengelolaan arsip;
- akses ruang arsip harus menggunakan PIN;
- penggunaan CCTV.

5. Nilai Risiko Yang Diharapkan

Atas semua aset yang teridentifikasi sebaiknya Bank menentukan nilai risiko yang diharapkan (limit risiko). Sebagai contoh apabila diharapkan risiko kebocoran informasi rahasia nasabah harus pada level low maka pada kolom 11 diisi **Low**.

6. Analisis Nilai Risiko

Dengan demikian, setelah semua langkah-langkah di atas dilakukan, maka contoh pengisian Form *Risk Register* adalah sbb :

Aset	Deskripsi Risiko	Analisa Kerawanan	Inheren			Kontrol yang Ada	Residual			Nilai Risiko Diharapkan
			Kecenderungan (min = 1, maks = 5)	Dampak (min = 1, maks = 5)	Nilai Risiko Dasar		Kecenderungan (min = 1, maks = 5)	Dampak (min = 1, maks = 5)	Nilai Risiko Akhir	
1	2	3	4	5	6	7	8	9	10	11
Informasi nasabah dalam bentuk hardcopy	Informasi bocor pada pihak yang tidak berwenang	Pengamanan terhadap lemari penyimpanan arsip kurang memadai	Level 4	Level 5	HIGH	- Ketentuan mengenai pengelolaan arsip - Akses ruang arsip dengan PIN - CCTV	Level 3	Level 2	MEDIUM	LOW
		Informasi nasabah diletakan terbuka (tercecer)								

Setelah form *Risk Register* terisi Bank melakukan analisis nilai risiko atas masing-masing aset yang teridentifikasi. Perbedaan antara NRD *High* dengan NRA *Medium* menunjukkan berkurangnya kecenderungan terjadinya risiko dan dampak yang ditimbulkan bila risiko terjadi tidak akan sebesar apabila pengendalian (*risk control system*) tidak diterapkan. Bank harus menganalisa apakah terdapat risiko yang belum dikendalikan namun dapat diterapkan bentuk pengendalian tertentu. Perbandingan antara NRA dengan Nilai Risiko yang diharapkan dari berbagai aset yang teridentifikasi merupakan parameter dasar untuk langkah-langkah yang diperlukan memitigasi risiko. Sebagai contoh apabila diharapkan risiko kebocoran informasi rahasia nasabah harus pada level *Low*, maka perlu dilakukan pengendalian tambahan apabila Nilai Risiko Akhir-nya masih *Medium* Bank selanjutnya menetapkan Rencana Penanganan Risiko atas aset tersebut. Misalnya Bank perlu memperbaiki *risk control system* untuk pengamanan informasi, mengkinikan kebijakan dan prosedur pengamanan.

**Lampiran 1.2****KATEGORI RISIKO PADA EUC**

Contoh kategori tingkat risiko suatu aplikasi atau suatu kegiatan untuk EUC:

Peringkat Risiko	Kategori Risiko	Tingkat Kekritisitas Bisnis dan Klasifikasi Data
5.	Sangat Tinggi	<ul style="list-style-type: none">• Dapat menimbulkan kerugian finansial yang sangat besar• Dapat memberikan dampak yang merugikan nilai Bank, termasuk harga saham (untuk Bank yang sudah Go-Publik)• Dapat menimbulkan sanksi dari Bank Indonesia• Memiliki dampak potensial atau aktual terhadap reputasi Bank secara internasional• Kegagalan memenuhi prinsip <i>corporate governance</i> yang sangat serius
4.	Tinggi	<ul style="list-style-type: none">• Dapat menimbulkan kerugian finansial yang besar• Dapat memberikan dampak yang serius bagi Bank• Dapat menimbulkan sanksi dari Bank Indonesia• Kemungkinan timbulnya sorotan publik (<i>reputation risk exposures</i>) apabila tidak ditangani secara benar• Isu pelayanan nasabah (<i>customer service</i>) yang berdampak serius terhadap bisnis Bank• Risiko reputasi amat potensial bagi Bank• Kegagalan memenuhi prinsip <i>corporate governance</i> yang cukup serius
3.	Menengah	<ul style="list-style-type: none">• Kerugian finansial yang dapat ditimbulkan cukup besar• Dampak yang cukup signifikan bagi bisnis Bank• Kemungkinan risiko reputasi pada skala menengah• Kegagalan memenuhi prinsip <i>corporate governance</i>
2.	Rendah	<ul style="list-style-type: none">• Kerugian finansial yang dapat ditimbulkan relatif rendah• Dampak terhadap bisnis Bank relatif kecil• Tidak ada sanksi dari Bank Indonesia• Risiko reputasi bagi Bank relatif rendah
1.	Dapat Diabaikan	<ul style="list-style-type: none">• Tidak ada /kecil dampak kerugian finansial bagi Bank• Dampak kerugian hanya terbatas pada unit bisnis pengguna aplikasi tersebut• Tidak ada risiko reputasi bagi Bank

Tabel diatas hanya merupakan contoh. Bank hendaknya membuat kriteria risiko yang disesuaikan dengan ukuran dan kompleksitas usaha Bank yang bersangkutan.



Lampiran 2

FORMULIR
PELAPORAN DAN PERMOHONAN
PERSETUJUAN PENGGUNAAN
TEKNOLOGI INFORMASI



DAFTAR ISI

Lampiran 2.1 Laporan Penggunaan Teknologi Informasi

Lampiran 2.1.1	Manajemen
Lampiran 2.1.2	Aplikasi dan Pengembangan
Lampiran 2.1.3	Operasional Teknologi Informasi
Lampiran 2.1.4	Jaringan Komunikasi
Lampiran 2.1.5	Pengamanan Informasi
Lampiran 2.1.6	<i>Business Continuity Plan</i>
Lampiran 2.1.7	<i>End User Computing</i>
Lampiran 2.1.8	<i>Electronic Banking</i>
Lampiran 2.1.9	Audit Teknologi Informasi (Audit TI)
Lampiran 2.1.10	Penyelenggaraan TI oleh Pihak Lain

Lampiran 2.2 Rencana Perubahan Mendasar Dalam Penggunaan Teknologi Informasi

Lampiran 2.2.1	Rencana Penerbitan <i>Electronic Banking</i> Transaksional
Lampiran 2.2.2	Rencana Penyelenggaraan <i>Data Center</i> dan atau <i>Disaster Recovery Center</i> oleh Pihak Lain di Dalam Negeri
Lampiran 2.2.3	Rencana Penyelenggaraan <i>Data Center</i> dan atau <i>Disaster Recovery Center</i> oleh Pihak Lain di Luar Negeri
Lampiran 2.2.4	Rencana Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Dalam Negeri
Lampiran 2.2.5	Rencana Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Luar Negeri

Lampiran 2.3 Laporan Realisasi Perubahan Mendasar Dalam Penggunaan Teknologi Informasi

Lampiran 2.3.1	Realisasi Penerbitan <i>Electronic Banking</i> Transaksional
Lampiran 2.3.2	Realisasi Penyelenggaraan <i>Data Center</i> dan atau <i>Disaster Recovery Center</i> oleh Pihak Lain di Dalam Negeri
Lampiran 2.3.3	Realisasi Penyelenggaraan <i>Data Center</i> dan <i>Disaster Recovery Center</i> oleh Pihak Lain di Luar Negeri
Lampiran 2.3.4	Realisasi Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Dalam Negeri



Lampiran 2.3.5 Realisasi Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Luar Negeri

Lampiran 2.4 Laporan Tahunan Penggunaan Teknologi Informasi

Lampiran 2.5 Laporan Kejadian Kritis, Penyalahgunaan dan/atau Kejahatan dalam Penyelenggaraan Teknologi Informasi (TI)

Lampiran 2.6 Permohonan Persetujuan Ulang Penyelenggaraan *Data Center* Dan Atau *Disaster Recovery Center* oleh Pihak Lain di Luar Negeri bagi Kantor Cabang Bank Asing



PENJELASAN CARA PENGISIAN LAPORAN

Petunjuk pengisian Laporan Penggunaan Teknologi Informasi, Laporan Tahunan Penggunaan Teknologi Informasi dan Laporan Kejadian Kritis.

Berilah tanda "V" jawaban yang sesuai :

Contoh:

V	ada	Tidak Ada	
---	-----	-----------	--

atau

	Ya	Tidak	V
--	----	-------	---

Apabila terdapat permintaan informasi dan dokumen pendukung, selain memberi tanda "V" maka Bank hendaknya memberikan informasi tersebut. Jika diperlukan, dapat menggunakan lembar tambahan untuk melengkapi penjelasan pada formulir yang diminta.

Apabila terdapat pertanyaan yang diikuti:

V	Terlampir	Tidak Terlampir	
---	-----------	-----------------	--

maka Bank memberi tanda "V" pada kotak "terlampir" apabila Bank menyertakan lampiran yang diminta pada laporan tersebut.

Untuk Laporan Penggunaan Teknologi Informasi, Laporan Tahunan dan Laporan Kejadian Kritis apabila Bank mencoret tanda "V" pada kotak "Tidak Terlampir" maka dianggap Bank tidak memiliki hal yang diminta untuk dilampirkan.

Apabila Bank dalam menyampaikan Laporan Tahunan Penggunaan Teknologi Informasi memberi tanda "V" pada kotak "Ada" untuk perubahan dan memberi tanda "V" pada kotak "Belum" untuk pelaporannya,

	Sudah	Belum	V
--	-------	-------	---

maka Bank harus memberikan data dan penjelasan mengenai perubahan tersebut. Bank dapat menggunakan lampiran terkait pada Laporan Penggunaan Teknologi Informasi yang disebutkan dimasing-masing nomor atau format bebas sesuai hal yang akan dilaporkan oleh bank.

Apabila Bank menggunakan lampiran pada Laporan Penggunaan Teknologi Informasi yang disebutkan maka tanda "V" yang tertera pada kotak "Tidak Terlampir" di lampiran tersebut, akan dianggap sebagai "tidak terdapat perubahan dari laporan sebelumnya.

	Terlampir	Tidak Terlampir	V
--	-----------	-----------------	---

Petunjuk Pengisian Laporan Perubahan Mendasar.

Setiap rencana perubahan yang mendasar dilaporkan dengan menggunakan Lampiran 2.2.. Apabila perubahan mendasar yang akan dilakukan merupakan penerbitan produk electronic banking dan atau penggunaan pihak penyedia jasa Teknologi Informasi maka dokumen yang harus disampaikan mengacu kepada lampiran terkait yang disebutkan pada Surat Edaran Ekstern. Bank mengisi kotak " Ya - Dokumen Terlampir" di kategori



perubahan mendasar yang dilaporkan dengan nomor lampiran terkait perubahan yaitu Lampiran 2.2.1. untuk rencana penerbitan produk electronic banking baru dan Lampiran 2.2.2., Lampiran 2.2.3, Lampiran 2.2.4 atau 2.2.5 untuk rencana penggunaan pihak penyedia jasa. Bank memberikan tanda "V" pada kotak "Tidak" di kategori lainnya/di luar yang dilaporkan.

Contoh apabila yang dilaporkan adalah rencana produk electronic banking baru:

Pertanyaan	Ya Dokumen Terlampir ^{***)}	Tidak ^{**)}	Keterangan
1. Konfigurasi / cara pengoperasian ^{***)}		V	
2. Sistem aplikasi <i>core banking</i> ^{****)}		V	
3. Produk <i>electronic banking</i> transaksional baru	Lampiran 2.2.1		
4. Penyelenggaraan TI oleh pihak lain		V	
5. Perubahan Mendasar Lain Menurut Bank yaitu : a. b.		V	

Format Laporan Perubahan Mendasar ini juga berlaku untuk lampiran permohonan persetujuan Bank Indonesia atas rencana Bank menggunakan pihak penyedia jasa di luar negeri untuk *Data Center*, *Disaster Recovery Center* atau Pemrosesan Transaksi Berbasis Teknologi Informasi.



Lampiran 2-1

**LAPORAN PENGGUNAAN TEKNOLOGI
INFORMASI**

Nama Bank
Alamat Kantor Pusat Bank
No. Telp.

Nama Penanggung Jawab
Kantor/Divisi/Bagian Penanggung
Jawab
Alamat Penanggung Jawab
No. Telp.

Tanggal Laporan _ _ _ _ _



Lampiran 2.1.1

MANAJEMEN

1. Struktur Organisasi Bank yang menunjukkan posisi Organisasi Teknologi Informasi^{*)}.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
2. Struktur Organisasi khusus satuan kerja Teknologi Informasi^{*)}.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
3. *IT Steering Committee (ITSC)*.
 - a. Surat Keputusan Pembentukan.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
 - b. Surat Keputusan/Risalah Rapat ITSC terakhir.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
4. Rencana jangka panjang (*IT Strategic Plan*)

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
5. *Job description* personil TI.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
6. *Training* di bidang TI yang pernah diikuti personil TI.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
7. *Risk Management*.
 - a. Terdapat petugas untuk memonitor risiko terkait TI.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
 - b. Terdapat *tools, system &* prosedur untuk memonitor risiko terkait TI baik di satuan kerja TI maupun satuan kerja pengguna TI.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
 - c. Terdapat analisis terkini dari *risk identification, risk measurement, risk monitoring and mitigation* dalam penyelenggaraan dan penggunaan Teknologi Informasi

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, lampirkan ringkasan analisis terkini tersebut

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

*) Struktur organisasi berdasarkan nama jabatan, baik di divisi TI maupun divisi pengguna utama TI, serta struktur organisasi berdasarkan nama pejabat di divisi TI mulai dari direksi penanggung jawab TI sampai kepala seksi.



Lampiran 2.1.2

APLIKASI DAN PENGEMBANGAN

1. Kebijakan, sistem & prosedur pengembangan aplikasi yang dilakukan bank.

	Ada	Tidak Ada	
--	-----	-----------	--

2. Daftar aplikasi yang sudah operasional^{*)}.
 - a. Dikembangkan sendiri.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--

 - b. Dikembangkan pihak penyedia jasa.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--

3. *Application Architecture*.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--

4. Daftar aplikasi yang sedang dalam pengembangan^{*)}.
 - a. Dikembangkan sendiri.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--

 - b. Dikembangkan pihak penyedia jasa.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--

5. Apakah bank memiliki fungsi *Project Management* untuk aplikasi yang sedang dalam pengembangan.

	Ya	Tidak	
--	----	-------	--

6. Apakah bank memisahkan *environment* untuk pengembangan, *testing* dan *production* ?

	Ya	Tidak	
--	----	-------	--

7. Apakah bank menggunakan *change control software*?

	Ya	Tidak	
--	----	-------	--

^{*)} Memuat informasi nama aplikasi, kegunaan, pihak pengembang (*in house* atau nama vendor), penyelenggara (*intern/outsourcing*), *platform*, tahun implementasi, *technical user documentation*, jenis *database system*, lokasi Server utama dan lokasi *server back up* yang meng-install aplikasi ini.



Lampiran 2.1.3

OPERASIONAL TEKNOLOGI INFORMASI

1. Informasi mengenai Pusat Data (*Data Center*) Bank :
 - a. Alamat
 - b. Status kepemilikan

<input type="checkbox"/>	Milik Sendiri	Milik penyedia jasa	<input type="checkbox"/>
--------------------------	---------------	---------------------	--------------------------
 - c. Spesifikasi server utama dan perangkat keras lainnya.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
 - d. Kelengkapan pengamanan fisik pada *Data Center*.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------
2. Apakah terdapat server yang ditempatkan di luar *data center* ?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
3. Aplikasi khusus untuk pengamanan informasi (*access control software*).

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
4. Prosedur Penanganan Masalah (*Problem Handling* termasuk *Helpdesk*).

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
5. Kebijakan, sistem & prosedur *change management*.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
6. Kebijakan, sistem dan prosedur pengelolaan hak akses pengguna sistem dan aplikasi

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
7. Penetapan sistem & *data sensitivity*

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
8. Ketersediaan *audit trail* pada sistem dan data.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------
9. Kebijakan, sistem dan prosedur *back up data*

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

*) Bila terdapat lebih dari 1 *data center*, misalnya ada *data center* khusus untuk treasury atau khusus untuk *trade finance* agar dicantumkan pula kelengkapan informasi *data center* lainnya dari no. 1 sampai dengan No. 9 diatas.



Lampiran 2.1.4

JARINGAN KOMUNIKASI

1. Arsitektur Jaringan Komunikasi Data (utama dan *back up*).

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

2. Kebijakan, sistem dan prosedur pengamanan jaringan.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

3. Daftar perangkat keras dan lunak yang digunakan untuk jaringan.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

4. *Network Monitoring System*.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

5. Kebijakan untuk konfigurasi pengamanan komunikasi data (misalnya *firewall*).

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------



Lampiran 2.1.5

PENGAMANAN INFORMASI ^{*)}

1. Kebijakan dan prosedur pengamanan informasi, mencakup antara lain:
 - a. Pemberian, perubahan & penghapusan akses *user*.

	Ada	Tidak Ada	
--	-----	-----------	--
 - b. *Security Awareness Program*.

	Ada	Tidak Ada	
--	-----	-----------	--
 - c. *Incident handling/Incident respond team*.

	Ada	Tidak Ada	
--	-----	-----------	--
 - d. Klasifikasi data.

	Ada	Tidak Ada	
--	-----	-----------	--
 - e. Penggunaan *emergency user ID*.

	Ada	Tidak Ada	
--	-----	-----------	--
 - f. Pencegahan penggunaan *software illegal*.

	Ada	Tidak Ada	
--	-----	-----------	--
2. Pengelolaan aset
 - a. Pengelolaan aset terkait informasi meliputi identifikasi, penentuan kepemilikan & tanggung jawab serta inventarisasi daftar aset.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--
 - b. Klasifikasi informasi (misalnya sangat rahasia, rahasia, biasa) dan prosedur pengamanannya.

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--
 - c. Pengamanan fisik termasuk penggunaan alat pengamanan (access control card, PIN dsb) terhadap fasilitas pemrosesan informasi.

	Ada	Tidak Ada	
--	-----	-----------	--
3. Pengamanan Akses
 - a. Penerapan pengamanan *password* pada aplikasi, misalnya aplikasi telah memaksa *user* untuk mengubah *password* secara berkala.

	Ada	Tidak ada	
--	-----	-----------	--

*) Bila bank menggunakan jasa pihak lain dalam penyelenggaraan TI, pertanyaan-pertanyaan di atas berlaku juga untuk penyelenggaraan TI tersebut.



- b. *Security Matrix* yang menjelaskan hak akses yang diberikan kepada masing-masing user untuk setiap aplikasi yang dimiliki Bank.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
- c. Terdapat fungsi audit (*audit log/audit trail*) untuk setiap aktivitas yang dilakukan oleh user dan dilakukan analisa terhadap *audit log* tersebut.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
- d. *Review* secara periodik terhadap kesesuaian antara *user* berikut hak akses yang diberikan oleh pihak yang independen.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
4. Sumber Daya Manusia
- a. Pencantuman ketentuan mengenai pengamanan informasi di dalam perjanjian dengan pegawai bank, pegawai kontrak dan pihak ketiga.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
- b. Adanya ketentuan mengenai sanksi atas pelanggaran terhadap kebijakan pengamanan informasi.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
- c. Prosedur pengembalian atau perubahan hak akses terhadap aset terkait informasi saat terjadi mutasi atau selesainya perjanjian kerja atau masa tugas.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
5. Pengamanan fisik termasuk penggunaan alat pengamanan (*access control card*, PIN dsb) terhadap fasilitas pemrosesan informasi.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
6. Operasional Aplikasi
Ketentuan tentang pengamanan dalam identifikasi dan otentikasi akses misalnya penggunaan, *password*, *token*, *biometric* dll.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
7. Penanganan Insiden Pengamanan Informasi
- a. Ketentuan mengenai keharusan untuk melaporkan terjadinya insiden pengamanan informasi.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|
- b. Prosedur mengenai pelaporan, penanganan, pendokumentasian dan tindak lanjut terjadinya insiden pengamanan informasi.
- | | | | |
|--------------------------|-----|-----------|--------------------------|
| <input type="checkbox"/> | Ada | Tidak ada | <input type="checkbox"/> |
|--------------------------|-----|-----------|--------------------------|



Lampiran 2.1.6

BUSINESS CONTINUITY PLAN

1. Kebijakan, sistem dan prosedur *Business Continuity Plan* termasuk *Disaster Recovery Plan* didalamnya.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila tidak ada, apakah Bank memiliki *Disaster Recovery Plan*?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

2. Struktur organisasi dan kewenangan *Business Continuity Plan*.*)

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

3. a. *Business Impact Analysis* terakhir.

Tgl

- b. *Risk Assessment Review* terakhir.

Tgl

4. *Disaster Recovery Center*

- a. Alamat

- b. Spesifikasi *back up server* dan perangkat keras lainnya.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

- c. Kelengkapan pengamanan fisik pada DRC.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

- d. Konfigurasi DRC (topologi jaringan, hardware, software, dan pendukung lainnya)

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

- e. *Back Up Data (hot, warm, cold back up)* untuk masing-masing aplikasi yang tersedia di DRC.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

5. Testing BCP & DRP.

- a. Kebijakan, sistem dan prosedur testing

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

- b. Pengujian menyeluruh (*overall testing*) atas seluruh sistem/aplikasi yang *critical* terakhir

Tgl

- c. Pengujian parsial dalam 1 (satu) tahun terakhir

Aplikasi	Tgl.....
Wilayah operasi.....	Tgl

*) Termasuk nama dan jabatan orang yang ada di dalam core team BCP



Lampiran 2.1.7

END USER COMPUTING

1. Daftar aplikasi yang dikembangkan dan/atau diadakan oleh unit kerja diluar unit kerja Teknologi Informasi.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

2. Apakah terdapat kebijakan dan prosedur yang telah disetujui Direksi dan Dewan Komisaris mengenai pengembangan dan pemeliharaan aplikasi oleh pengguna akhir.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------



Lampiran 2.1.8

ELECTRONIC BANKING

1. Produk *e-banking* yang disediakan bank (jawaban dapat lebih dari satu):

a. Kartu ATM

<input type="checkbox"/>	Ya	<input type="checkbox"/>	Tidak	<input type="checkbox"/>
--------------------------	----	--------------------------	-------	--------------------------

Jenis rekening terkait:

<input type="checkbox"/>	Giro	<input type="checkbox"/>	Tabungan	<input type="checkbox"/>	Kredit	<input type="checkbox"/>	Deposito	<input type="checkbox"/>	Lainnya
--------------------------	------	--------------------------	----------	--------------------------	--------	--------------------------	----------	--------------------------	---------

b. Kartu Debit

<input type="checkbox"/>	Ya	<input type="checkbox"/>	Tidak	<input type="checkbox"/>
--------------------------	----	--------------------------	-------	--------------------------

Jenis rekening terkait:

<input type="checkbox"/>	Giro	<input type="checkbox"/>	Tabungan	<input type="checkbox"/>	Kredit	<input type="checkbox"/>	Deposito	<input type="checkbox"/>	Lainnya
--------------------------	------	--------------------------	----------	--------------------------	--------	--------------------------	----------	--------------------------	---------

c. Kartu Kredit

<input type="checkbox"/>	Ya	<input type="checkbox"/>	Tidak	<input type="checkbox"/>
--------------------------	----	--------------------------	-------	--------------------------

d. Kartu Prabayar yang dapat diisi ulang (*prepaid card*).

<input type="checkbox"/>	Ya	<input type="checkbox"/>	Tidak	<input type="checkbox"/>
--------------------------	----	--------------------------	-------	--------------------------

e. *SMS Banking*

<input type="checkbox"/>	Ya			<input type="checkbox"/>	Tidak	<input type="checkbox"/>
	<i>Informational</i>	<input type="checkbox"/>	<i>Communicative</i>			

f. *Internet Banking*

<input type="checkbox"/>	Ya			<input type="checkbox"/>	Tidak	<input type="checkbox"/>
	<i>Informational</i>	<input type="checkbox"/>	<i>Communicative</i>			

g. *Phone Banking*

<input type="checkbox"/>	Ya			<input type="checkbox"/>	Tidak	<input type="checkbox"/>
	<i>Informational</i>	<input type="checkbox"/>	<i>Communicative</i>			

h. Produk lain yaitu

2. Bekerjasama dengan perusahaan/bank lain (*principal, acquirer, switching company*)

<input type="checkbox"/>	Ya	<input type="checkbox"/>	Tidak	<input type="checkbox"/>
--------------------------	----	--------------------------	-------	--------------------------

3. Apakah terdapat kebijakan dan prosedur terkait setiap produk *e-banking* yang telah disetujui Direksi dan Dewan Komisaris.

<input type="checkbox"/>	Ada	<input type="checkbox"/>	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	--------------------------	-----------	--------------------------



4. a. Sistem arsitektur TI untuk masing-masing produk *e-banking* dan bentuk koneksi dengan *core banking system*;

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

- b. Sistem pengamanan (mencakup *confidentiality, integrity, availability* dan *authentication*) yang digunakan pada masing-masing produk *e-banking*

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

5. Apakah terdapat analisis terkini dalam 1 (satu) tahun terakhir dari *risk identification, risk measurement, risk monitoring and mitigation* untuk setiap produk *e-banking*.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada:

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

6. Apakah terdapat program edukasi dan mekanisme perlindungan nasabah untuk setiap produk *e-banking*.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

7. Data Statistik Transaksi *e-banking* selama 1 (satu) tahun kalender terakhir

Nama Produk	Jenis Data	Jumlah
<i>Phone Banking</i>	Jumlah Nasabah	
	Nilai Transaksi	Rp.....juta
	Frekuensi Transaksi	
<i>SMS/Mobile Banking</i>	Jumlah Nasabah	
	Nilai Transaksi	Rp.....juta
	Frekuensi Transaksi	
<i>Internet Banking</i>	Jumlah Nasabah	
	Nilai Transaksi	Rp.....juta
	Frekuensi Transaksi	
<i>Prepaid Card</i>	Jumlah Nasabah	
	Nilai Transaksi	Rp.....juta
	Frekuensi Transaksi	



Lampiran 2.1.9

AUDIT TEKNOLOGI INFORMASI (AUDIT TI)*)

1. Bank memiliki unit kerja atau personil untuk audit intern khusus TI.
- | | | | |
|--------------------------|----|-------|--------------------------|
| <input type="checkbox"/> | Ya | Tidak | <input type="checkbox"/> |
|--------------------------|----|-------|--------------------------|

Jika ya, lampirkan struktur organisasi Audit TI dan lengkapi dengan *curriculum vitae* auditor intern.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

2. Jika jawaban pada no. 1 adalah tidak, apakah bank menggunakan auditor ekstern untuk melakukan audit intern khusus TI?

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

Jika ya, lampirkan perjanjian kerja terkini.

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

3. *Review* terakhir oleh pihak independen terhadap fungsi audit intern TI.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

4. Bank memiliki pedoman Audit Intern TI.

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

5. Audit khusus TI dilaksanakan minimal 1 kali setahun.

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

6. Apakah audit khusus pada nomor 5 juga dilakukan atas *Data Center, Disaster Recovery Center* dan Pemrosesan Transaksi Berbasis TI yang diselenggarakan oleh pihak lain?

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

Bila ya, sebutkan dua tanggal audit TI terakhir.

Tgl

Tgl

7. Apakah audit khusus TI tersebut di atas, dalam 3 tahun terakhir telah mencakup seluruh modul dalam aplikasi *Core Banking*?

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

8. Laporan Audit khusus TI termasuk yang dilaporkan kepada Komite Audit.

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

*) Informasi mencakup jenis layanan, data penyedia jasa (nama perusahaan, alamat *data center*, 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 .



Lampiran 2.1.10

PENYELENGGARAAN TI OLEH PIHAK LAIN

1. Daftar layanan TI yang diselenggarakan oleh pihak ketiga diluar pengembangan sistem aplikasi*).

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

2. Copy perjanjian antara bank dengan penyelenggara Data Center, *Disaster Recovery Center* dan Pemrosesan transaksi berbasis TI

<input type="checkbox"/>	Terlampir	Tidak Terlampir	<input type="checkbox"/>
--------------------------	-----------	-----------------	--------------------------

3. Hasil *review* terkini mengenai analisis biaya & manfaat penyelenggaraan TI oleh pihak lain yang antara lain mencakup:

- a. manfaat bagi Bank melampaui biaya dibebankan oleh pihak penyedia jasa kepada Bank;
- b. Penilaian kecukupan dan kesesuaian sistem aplikasi yang digunakan dengan kebutuhan bank;
- c. Analisis sistem pengamanan yang digunakan oleh pihak penyedia jasa.

<input type="checkbox"/>	Ada	Tidak ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

4. Analisis bank mengenai kecukupan *Disaster Recovery Plan* milik pihak penyedia jasa penyelenggara TI.

<input type="checkbox"/>	Ada	Tidak ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

5. Analisis kelangsungan penyediaan jasa berdasarkan kinerja terkini perusahaan penyedia jasa termasuk laporan keuangan dan risiko yang terkait antara lain risiko operasional, hukum dan reputasi dari perusahaan penyedia jasa.

<input type="checkbox"/>	Ada	Tidak ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

6. a. Apakah penyelenggaraan *Data Center*, *Disaster Recovery Center* dan Pemrosesan transaksi berbasis TI oleh pihak lain dilakukan audit TI oleh auditor ekstern Bank?

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

- b. Bila ya, sebutkan dua tanggal audit TI terakhir.
 Tgl
 Tgl

- c. Apakah dilakukan audit TI oleh auditor ekstern pihak penyedia jasa?

<input type="checkbox"/>	Ya	Tidak	<input type="checkbox"/>
--------------------------	----	-------	--------------------------

- d. Bila ya, sebutkan dua tanggal audit TI terakhir.
 Tgl
 Tgl



Lampiran 2-2

**RENCANA PERUBAHAN MENDASAR DALAM
PENGUNAAN TEKNOLOGI INFORMASI*)**

Nama Bank ----- Alamat Kantor Pusat Bank ----- No. Telp. -----
Nama Pelapor ----- Kantor/Divisi/Bagian Pelapor ----- Alamat Pelapor ----- No. Telp. -----
Tanggal Laporan _ _ _ _ _

Apakah terdapat **rencana** perubahan mendasar dalam penyelenggaraan Teknologi Informasi?

Pertanyaan	Ya Dokumen Terlampir**)	Tidak **)	Keterangan
6. Konfigurasi / cara pengoperasian ***)			
7. Sistem aplikasi <i>core banking</i> ****)			
8. Produk <i>electronic banking</i> transaksional baru			
9. Penyelenggaraan TI oleh pihak lain			
10. Perubahan Mendasar Lain Menurut Bank yaitu : a.			

*) Perubahan dalam penyelenggaraan TI dilaporkan 2 (dua) bulan sebelum rencana perubahan tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI dan SE. Penyelenggaraan TI oleh pihak lain di luar negeri hanya dapat dilakukan setelah memperoleh persetujuan Bank Indonesia.

***) Cantumkan apakah dokumen pendukung yang harus disampaikan telah dilampirkan. Dokumen pendukung tersebut mengacu pada Lampiran 2.2.1 untuk produk *electronic banking* baru dan lampiran 2.2.2, 2.2.3, 2.2.4 atau 2.2.5 untuk penyelenggaraan TI oleh pihak ketiga, sedangkan untuk perubahan mendasar yang lainnya format bebas.

****) Yang dimaksud dengan perubahan terhadap konfigurasi antara lain topologi/arsitektur TI Bank, *platform/operating system*, *server* utama terkait dengan aplikasi *core banking*, baik yang diselenggarakan sendiri maupun menggunakan jasa pihak penyedia jasa Teknologi Informasi.

*****) Yang dimaksud dengan Aplikasi *core banking* adalah sistem aplikasi untuk memproses dan mengolah data terkait produk dan jasa utama Bank, yang jika tidak berfungsi akan mengganggu keberlangsungan usaha dan menimbulkan kerugian yang signifikan bagi Bank.



Lampiran 2.2.1

**RENCANA PENERBITAN
ELECTRONIC BANKING TRANSAKSIONAL^{*)}**

1. Sistem, prosedur dan kewenangan dalam penerbitan produk *Electronic Banking*.
2. Uraian singkat atau penjelasan mengenai produk *e-banking* yang akan diterbitkan.
3. Kebijakan dan prosedur yang menjelaskan kesiapan infrastruktur Teknologi Informasi masing-masing produk *Electronic Banking*.
4. Lampirkan penjelasan mengenai sistem arsitektur Teknologi Informasi dari produk *e-banking* yang akan diterbitkan dan bentuk koneksi dengan *core banking system*.
5. Hasil analisis dan identifikasi risiko pada Bank terhadap risiko yang melekat pada produk *electronic banking* dan bentuk pengendalian pengamanan untuk mitigasi risiko tersebut antara lain untuk memastikan terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), otentifikasi (*authentication*) dan ketersediaan (*availability*).
6. Jelaskan secara tersendiri aturan yang diterapkan bank mengenai:
 - a. 2 faktor authentication yang akan digunakan;
 - b. Encryption yang akan digunakan;
 - c. Password (kriteria numeric alphanumeric, panjang password).
7. Uraian sistem informasi akuntansi yang akan diterapkan untuk produk yang akan diterbitkan.
8. Lampirkan hasil analisis dan identifikasi risiko produk *e-banking* antara lain risiko operasional, hukum dan reputasi.
9. Lampirkan hasil pemeriksaan pihak independen yang memberikan pendapat atas karakteristik produk dan kecukupan pengamanan sistem TI terkait produk serta kepatuhan terhadap ketentuan dan/atau praktek-praktek yang berlaku di dunia internasional (*best practices*).
10. Uraian kesiapan struktur organisasi pendukung dan bentuk pengawasan yang melekat (*built in control*) yang akan diterapkan atas produk *e-banking* yang akan diterbitkan.
11. Hasil analisis bisnis mengenai proyeksi penerbitan produk baru dalam 1 (satu) tahun kedepan

^{*)} Rencana penerbitan *e-banking* dilaporkan 2 (dua) bulan sebelum rencana perubahan tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI.



Lampiran 2.2.2

**RENCANA PENYELENGGARAAN *DATA CENTER*
DAN ATAU *DISASTER RECOVERY CENTER* OLEH
PIHAK LAIN DI DALAM NEGERI^{*)}**

1. Rencana lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....

Lampirkan data nama dan alamat serta kepemilikan penyelenggara *Data center* dan atau *Disaster Recovery Center* yang direncanakan.

2. Lampirkan ringkasan hasil pendefinisian kebutuhan dan *due diligence* yang telah dilakukan Bank dalam rencana menggunakan penyedia jasa untuk menyelenggarakan *Data Center* dan atau *Disaster Recovery Center* di dalam negeri.
3. Berkaitan dengan ringkasan *due diligence* pada nomor 2, sertakan hal-hal dibawah ini sebagai lampiran ringkasan tersebut:
 - a. analisis Bank atas hasil audit teknologi informasi yang dilakukan oleh pihak independen terhadap pengembangan sistem aplikasi yang ditawarkan dan sistem pengamanan pada fasilitas yang dimiliki oleh pihak penyedia jasa;
 - b. analisis risiko Bank mengenai rencana menyerahkan penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* kepada pihak penyedia jasa antara lain risiko operasional, hukum dan reputasi;
 - c. analisis Bank mengenai kecukupan *Disaster Recovery Plan* milik pihak penyedia jasa penyelenggara TI.
4. Bila sudah ada lampirkan konsep perjanjian antara bank dengan penyelenggara TI yang memuat hal-hal sebagaimana dipersyaratkan dalam Peraturan Bank Indonesia. Bila konsep perjanjian belum ada lampirkan ringkasan proposal dari calon penyelenggara dan ringkasan analisis bank atas proposal tersebut.
5. Proposal pada nomor 4 mencakup ringkasan analisis risiko oleh pihak penyedia jasa penyelenggara TI atas penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* yang akan ditawarkan kepada bank.
6. Lampirkan ringkasan analisis biaya & manfaat penyelenggaraan TI oleh pihak lain yang antara lain mencakup:
 - a. penilaian kecukupan dan kesesuaian sistem aplikasi yang akan digunakan dengan kebutuhan bank;
 - b. analisis atas pengendalian pengamanan yang digunakan pihak penyedia jasa untuk memastikan terpenuhinya *confidentiality, integrity, availability* dan *authentication*;

^{*)} Rencana bank menggunakan pihak penyedia jasa dalam menyelenggarakan *data center* dan DRC di dalam negeri dilaporkan 2 (dua) bulan sebelum penyelenggaraan TI tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI.



- c. analisis kinerja, reputasi dan kelangsungan penyediaan layanan kepada para pengguna jasa.
7. Lampirkan gambar *IT Architecture* yang telah ada dan yang direncanakan setelah penyelenggaraan DC /DRC diserahkan kepada pihak penyedia jasa.
8. Lampirkan rencana pengawasan yang akan dilakukan bank atas penyelenggaraan *Data Center* dan atau *Disaster Recovery Center*.
9. Lampirkan Surat Pernyataan dari Bank mengenai kesediaan Bank memberikan akses kepada auditor intern, ekstern maupun Bank Indonesia untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.



Lampiran 2.2.3

**RENCANA PENYELENGGARAAN DATA CENTER DAN
ATAU DISASTER RECOVERY CENTER OLEH
PIHAK LAIN DI LUAR NEGERI^{*)}**

1. Rencana lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....

Lampirkan data nama dan alamat serta kepemilikan penyelenggara *Data center* dan atau *Disaster Recovery Center* yang direncanakan.
2. Lampirkan ringkasan hasil pendefinisian kebutuhan dan *due diligence* yang telah dilakukan Bank dalam rencana menggunakan penyedia jasa untuk menyelenggarakan *Data Center* dan atau *Disaster Recovery Center* di luar negeri.
3. Berkaitan dengan ringkasan *due diligence* pada nomor 2, sertakan hal-hal dibawah ini sebagai lampiran ringkasan tersebut:
 - a. analisis bank atas hasil audit teknologi informasi yang dilakukan oleh pihak independen terhadap pengembangan sistem aplikasi yang ditawarkan dan sistem pengamanan pada fasilitas yang dimiliki oleh pihak penyedia jasa;
 - b. analisis risiko Bank mengenai rencana menyerahkan penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* kepada pihak penyedia jasa antara lain risiko operasional, hukum dan reputasi serta analisis *country risk*;
 - c. analisis Bank mengenai kecukupan *Disaster Recovery Plan* milik pihak penyedia jasa penyelenggara TI.
4. Lampirkan konsep perjanjian antar bank dengan penyelenggara *Data Center* dan atau *Disaster Recovery Center* di luar negeri yang memuat hal-hal sebagaimana dipersyaratkan dalam Peraturan Bank Indonesia.
5. Lampirkan ringkasan analisis risiko oleh pihak penyedia jasa penyelenggara TI atas penyelenggaraan *Data center* dan atau *Disaster Recovery Center* yang akan ditawarkan kepada bank.
6. Lampirkan ringkasan analisis biaya & manfaat penyelenggaraan TI oleh pihak lain yang antara lain mencakup:
 - a. manfaat bagi Bank melampaui biaya dibebankan oleh pihak penyedia jasa kepada Bank;
 - b. penilaian kecukupan dan kesesuaian sistem aplikasi yang akan digunakan dengan kebutuhan bank;
 - c. analisis atas pengendalian pengamanan yang digunakan pihak penyedia jasa untuk memastikan terpenuhinya *confidentiality*, *integrity*, *availability* dan *authentication*;

^{*)} Permohonan Bank untuk izin menggunakan pihak penyedia jasa dalam menyelenggarakan *data center* dan DRC di luar negeri diajukan 4 (empat) bulan sebelum penyelenggaraan TI tersebut efektif dioperasikan untuk memperoleh persetujuan dari Bank Indonesia sebagaimana dipersyaratkan pada PBI



- d. analisis kinerja, reputasi dan kelangsungan penyediaan layanan kepada para pengguna jasa.
7. Lampirkan gambar *IT Architecture* sekarang dan yang direncanakan setelah penyelenggaraan DC /DRC diserahkan kepada pihak penyedia jasa.
8. Lampirkan rencana pengawasan yang akan dilakukan bank atas penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* yang direncanakan.
9. Lampirkan Surat Pernyataan dari Bank mengenai kesediaan Bank memberikan akses kepada auditor intern, ekstern maupun Bank Indonesia untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.
10. Bila Bank merupakan Kantor Cabang Bank Asing atau Bank yang dimiliki lembaga keuangan asing, lampirkan:
 - a. Surat Pernyataan dari otoritas pengawas lembaga keuangan di luar negeri bahwa pihak penyedia jasa merupakan cakupan pengawasannya;
 - b. Surat Pernyataan tidak keberatan dari otoritas pengawas setempat bila Bank Indonesia hendak melakukan pemeriksaan penyelenggaraan pusat data (*Data Center*) dan atau *Disaster Recovery Center* tersebut;
 - c. Surat Pernyataan bahwa Bank secara berkala akan menyampaikan hasil penilaian yang dilakukan kantor Bank di luar negeri atas penerapan manajemen risiko pada pihak penyedia jasa. Surat Pernyataan ini mencantumkan periodisasi yang direncanakan;
 - d. Hasil penilaian oleh kantor Bank di luar negeri atas penerapan manajemen risiko yang dilakukan oleh pihak penyedia jasa.
11. Lampirkan rencana Bank mengenai:
 - a. peningkatan kualitas pelayanan kepada nasabah;
 - b. peningkatan kemampuan sumber daya manusia yang berkaitan dengan penyelenggaraan TI yang digunakan oleh Bank.



Lampiran 2.2.4

**RENCANA PENYELENGGARAAN PEMROSESAN
TRANSAKSI BERBASIS TEKNOLOGI INFORMASI OLEH
PIHAK LAIN DI DALAM NEGERI^{*)}**

1. Aktivitas dan produk yang penyelenggaraannya akan diserahkan kepada pihak penyedia jasa termasuk uraian atau penjelasan dan flow chart dari prosedur pelaksanaan (SOP).
2. Lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....
 - c. pemrosesan transaksi.....

Lampirkan data nama dan alamat serta kepemilikan penyelenggara Pemrosesan Transaksi Berbasis Teknologi Informasi yang direncanakan.

3. Lampirkan ringkasan hasil pendefinisian kebutuhan dan *due dilligence* yang telah dilakukan Bank dalam rencana menggunakan penyedia jasa untuk menyelenggarakan Pemrosesan Transaksi Berbasis Teknologi Informasi di dalam negeri.
4. Berkaitan dengan ringkasan *due diligence* pada nomor 3, sertakan hal-hal dibawah ini sebagai lampiran ringkasan tersebut:
 - a. analisis bank atas hasil audit teknologi informasi yang dilakukan oleh pihak independen terhadap sumber daya TI (termasuk pengembangan sistem aplikasi yang ditawarkan, sistim operasi dan prosedur, dan sistem pengamanan pada fasilitas yang dimiliki) yang akan digunakan untuk memproses transaksi oleh pihak penyedia jasa;
 - b. analisis risiko Bank atas rencana menyerahkan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi kepada pihak penyedia jasa antara lain risiko operasional, hukum dan reputasi;
 - c. analisis Bank mengenai kecukupan *Disaster Recovery Plan* milik pihak penyedia jasa penyelenggara Pemrosesan Transaksi Berbasis Teknologi Informasi.
5. Bila sudah ada lampirkan konsep perjanjian antara bank dengan penyelenggara Pemrosesan Transaksi Berbasis Teknologi Informasi di dalam negeri , bila belum ada lampirkan ringkasan proposal dari calon penyelenggara dan ringkasan analisis bank atas proposal tersebut.

^{*)} Rencana Bank untuk menggunakan pihak penyedia jasa dalam menyelenggarakan pemrosesan transaksi berbasis teknologi informasi di dalam negeri dilaporkan 2 (dua) bulan sebelum penyelenggaraan pemrosesan transaksi berbasis teknologi informasi tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI



6. Proposal pada nomor 5 mencakup ringkasan analisis risiko oleh pihak penyedia jasa penyelenggara TI atas penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi yang akan ditawarkan kepada Bank.
7. Lampirkan ringkasan analisis biaya & manfaat penyelenggaraan TI oleh pihak lain yang antara lain mencakup:
 - a. penilaian kecukupan dan kesesuaian sistem aplikasi yang akan digunakan dengan kebutuhan Bank.
 - b. analisis Bank atas pengendalian pengamanan yang digunakan pihak penyedia jasa untuk memastikan terpenuhinya *confidentiality, integrity, availability* dan *authentication*.
 - c. analisis kinerja, reputasi dan kelangsungan penyediaan layanan kepada para pengguna jasa.
8. Lampirkan gambar garis pelaporan dan informasi sekarang dan yang direncanakan setelah penyelenggaraan pemrosesan transaksi diserahkan kepada pihak penyedia jasa.
9. Lampirkan rencana pengawasan yang akan dilakukan Bank atas penyelenggaraan Pemrosesan Transaksi Berbasis TI yang direncanakan.
10. Lampirkan Surat Pernyataan dari Bank mengenai kesediaan Bank memberikan akses kepada auditor intern, ekstern maupun Bank Indonesia untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.



Lampiran 2.2.5

**RENCANA PENYELENGGARAAN PEMROSESAN
TRANSAKSI BERBASIS TEKNOLOGI INFORMASI OLEH
PIHAK LAIN DI LUAR NEGERI^{*)}**

1. Aktivitas dan produk yang penyelenggaraannya akan diserahkan kepada pihak penyedia jasa termasuk uraian atau penjelasan dan *flow chart* dari prosedur pelaksanaan (SOP).
2. Lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....
 - c. pemrosesan transaksi

Lampirkan data nama dan alamat serta kepemilikan penyelenggara Pemrosesan Transaksi Berbasis TI yang direncanakan.

3. Lampirkan ringkasan hasil pendefinisian kebutuhan dan *due diligence* yang telah dilakukan Bank dalam rencana menggunakan penyedia jasa untuk menyelenggarakan Pemrosesan Transaksi Berbasis TI di Luar Negeri
4. Berkaitan dengan ringkasan *due diligence* pada nomor 3, sertakan hal-hal dibawah ini sebagai lampiran ringkasan tersebut:
 - a. analisis Bank atas hasil audit teknologi informasi 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 pihak penyedia jasa;
 - b. analisis risiko Bank atas rencana menyerahkan penyelenggaraan Pemrosesan Transaksi Berbasis TI kepada pihak penyedia jasa antara lain risiko operasional, hukum dan reputasi serta analisis *country risk*;
 - c. analisis Bank mengenai kecukupan *Disaster Recovery Plan* milik pihak penyedia jasa penyelenggara TI.
5. Lampirkan konsep perjanjian antara bank dengan penyelenggara Pemrosesan Transaksi Berbasis TI di luar negeri yang memuat hal-hal sebagaimana dipersyaratkan dalam Peraturan Bank Indonesia.
6. Lampirkan ringkasan analisis risiko oleh pihak penyedia jasa penyelenggara TI atas penyelenggaraan Pemrosesan Transaksi Berbasis TI yang akan ditawarkan kepada Bank.

^{*)} Permohonan Bank untuk izin menggunakan pihak penyedia jasa dalam menyelenggarakan pemrosesan transaksi berbasis teknologi informasi di luar negeri 4 (empat) bulan sebelum penyelenggaraan pemrosesan transaksi berbasis teknologi informasi tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI



7. Lampirkan ringkasan analisis biaya & manfaat penyelenggaraan Pemrosesan Transaksi Berbasis TI oleh pihak lain yang antara lain mencakup:
 - a. manfaat bagi Bank melampaui biaya dibebankan oleh pihak penyedia jasa 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 *confidentiality, integrity, availability* dan *authentication*.
 - d. analisis kinerja, reputasi dan kelangsungan penyediaan layanan kepada para pengguna jasa.
8. Lampirkan gambar garis pelaporan dan informasi sekarang dan yang direncanakan setelah pemrosesan transaksi diserahkan kepada pihak penyedia jasa.
9. Bila Bank merupakan Kantor Cabang Bank Asing atau Bank yang dimiliki lembaga keuangan asing, lampirkan:
 - a. Surat Pernyataan dari otoritas pengawas lembaga keuangan di luar negeri bahwa pihak penyedia jasa merupakan cakupan pengawasannya;
 - b. Surat Pernyataan tidak keberatan dari otoritas pengawas setempat bila Bank Indonesia hendak memeriksa penyelenggaraan Pemrosesan Transaksi Berbasis TI 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 pihak penyedia jasa. Surat Pernyataan ini mencantumkan periodisasi yang direncanakan.
 - d. Hasil penilaian oleh kantor Bank di luar negeri atas penerapan manajemen risiko yang dilakukan oleh pihak penyedia jasa.
10. Lampirkan rencana pengawasan yang akan dilakukan bank atas penyelenggaraan Pemrosesan Transaksi Berbasis TI yang direncanakan.
11. Lampirkan rencana Bank mengenai:
 - a. peningkatan kemampuan sumber daya manusia yang berkaitan dengan penyelenggaraan TI yang digunakan oleh Bank;
 - b. peningkatan kemampuan sumber daya manusia atas produk-produk yang ditawarkan Bank kepada nasabah;
 - c. penerapan aspek perlindungan kepada nasabah atas produk yang pemrosesannya diserahkan kepada pihak penyedia jasa;
 - 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 Bank Indonesia untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.



Lampiran 2-3

**REALISASI PERUBAHAN MENDASAR DALAM
PENGUNAAN TEKNOLOGI INFORMASI*)**

Nama Bank ----- Alamat Kantor Pusat Bank ----- No. Telp. -----
Nama Pelapor ----- Kantor/Divisi/Bagian Pelapor ----- Alamat Pelapor ----- No. Telp. -----
Tanggal Laporan _ _ _ _ _

Apakah terdapat realisasi perubahan mendasar dalam penyelenggaraan Teknologi Informasi?

Pertanyaan	Ya Dokumen Terlampir ^{**)}	Tidak	Keterangan
1. Konfigurasi / cara pengoperasian ^{***)}			
2. Sistem aplikasi <i>core banking</i> ^{****)}			
3. Produk <i>electronic banking</i> transaksional baru			
4. Penyelenggaraan TI oleh pihak Lain			
5. Perubahan Mendasar Lain Menurut Bank yaitu : a. b.			

*) Perubahan dalam penyelenggaraan TI dilaporkan 1 (satu) bulan setelah rencana perubahan tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI dan SE.

***) Cantumkan apakah dokumen pendukung yang harus disampaikan telah dilampirkan. Dokumen pendukung tersebut mengacu pada Lampiran 2.3.1 untuk produk *electronic banking* baru dan lampiran 2.3.2, 2.2.3, 2.2.4 atau 2.2.5 untuk penyelenggaraan TI oleh pihak ketiga sedangkan untuk yang lainnya format bebas.

****) Yang dimaksud dengan perubahan terhadap konfigurasi antara lain topologi/arsitektur TI Bank, *platform/operating system, server* utama terkait dengan aplikasi *core banking*, baik yang diselenggarakan sendiri maupun menggunakan jasa pihak penyedia jasa TI.

*****) Yang dimaksud dengan Aplikasi *core banking* adalah sistem aplikasi untuk memproses dan mengolah data terkait produk dan jasa utama Bank, yang jika tidak berfungsi akan mengganggu keberlangsungan usaha dan menimbulkan kerugian yang signifikan bagi Bank.



Lampiran 2.3.1

**REALISASI PENERBITAN
ELECTRONIC BANKING TRANSAKSIONAL^{*)}**

1. Uraian singkat atau penjelasan mengenai produk *e-banking* yang baru diterbitkan.
2. Lampirkan penjelasan mengenai sistem arsitektur TI dari produk *e-banking* yang baru diterbitkan. dan bentuk koneksi dengan *core banking system*.
3. Lampirkan penjelasan mengenai bentuk pengendalian intern khususnya pengendalian keamanan (memastikan terpenuhinya *confidentiality, integrity, availability* dan *authentication*).
4. Uraian kesiapan struktur organisasi pendukung dan bentuk pengawasan yang melekat (*built in control*) atas produk *e-banking*.
5. Lampirkan kebijakan dan prosedur yang menjelaskan kesiapan infrastruktur Teknologi Informasi dari produk *e-banking*.
6. Uraian sistem informasi akuntansi.
7. Lampirkan hasil analisis dan identifikasi risiko produk *e-banking* identifikasi, pengukuran, monitoring dan mitigasi risiko dari produk *e-banking* yang baru diterbitkan antara lain risiko operasional, hukum dan reputasi.
8. Lampirkan hasil *post implementation review* (PIR) atas penggunaan TI terkait produk *e-banking* yang baru diterbitkan, termasuk tapi tidak terbatas pada review mengenai:
 - a. System berjalan dengan baik (*system performance review*).
 - b. Komplain nasabah dan tindak lanjutnya.
 - c. Kesesuaian dengan user requirement
 - d. Problem yang terjadi dan solusi/eskalasi/penyelesaian yang dibuat
 - e. Efektifitas pengamanan yang ditetapkan

^{*)} Realisasi penerbitan produk *e-banking* dilaporkan 1 (satu) bulan setelah rencana perubahan tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI



Lampiran 2.3.2

**REALISASI PENYELENGGARAAN *DATA CENTER*
DAN ATAU *DISASTER RECOVERY CENTER*
OLEH PIHAK LAIN DI DALAM NEGERI^{*)}**

1. Lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....
2. Lampirkan *copy* perjanjian antar bank dengan penyelenggara TI.
3. Lampirkan hasil *post implementation review* (PIR) atas penggunaan *Data Center* pihak penyedia jasa yang antara lain mencakup review mengenai:
 - a. System berjalan dengan baik (system performance review)
 - b. Kesesuaian dengan user requirement
 - c. Problem yang terjadi dan solusi/eskalasi/penyelesaian yang dibuat
 - d. Efektifitas pengamanan yang ditetapkan
4. Lampirkan hasil pengujian/testing atas penggunaan *Disaster Recovery Center* yang diselenggarakan pihak penyedia jasa tersebut.
5. Lampirkan Berita Acara pengalihan *Data Center* dan/atau *Disaster Recovery Center*.
6. Lampirkan gambar IT Architecture setelah penyelenggaraan DC /DRC diserahkan kepada pihak penyedia jasa.
7. Uraian analisis risiko terkini penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* tersebut antara lain risiko operasional, hukum dan reputasi.

^{*)} Laporan penggunaan pihak penyedia jasa dalam menyelenggarakan *data center* dan DRC disampaikan Bank 1 (satu) bulan setelah penyelenggaraan TI tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI.



Lampiran 2.3.3

**REALISASI PENYELENGGARAAN *DATA CENTER*
DAN *DISASTER RECOVERY CENTER* OLEH
PIHAK LAIN DI LUAR NEGERI^{*)}**

1. Lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....
2. Lampirkan *copy* perjanjian antara bank dan penyelenggara *Data Center* dan atau *Disaster Recovery Center*.
3. Lampirkan hasil analisis terkini atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya *confidentiality*, *integrity*, *availability* dan *authentication* dalam penyelenggaraan yang diserahkan kepada pihak penyedia jasa.
4. Lampirkan hasil *post implementation review* (PIR) atas penggunaan *Data Center* pihak penyedia jasa yang antara lain mencakup review mengenai:
 - a. system berjalan dengan baik (system performance review);
 - b. kesesuaian dengan user requirement;
 - c. problem yang terjadi dan solusi/eskalasi/penyelesaian yang dibuat;
 - d. efektifitas pengamanan yang ditetapkan.
5. Lampirkan hasil pengujian/*testing* atas penggunaan *Disaster Recovery Center* yang diselenggarakan pihak penyedia jasa tersebut.
6. Lampirkan Berita Acara pengalihan *Data Center* dan/atau *Disaster Recovery Center*.
7. Lampirkan gambar IT Architecture sekarang setelah penyelenggaraan DC /DRC diserahkan kepada pihak penyedia jasa.
8. Uraian analisis risiko terkini Bank terhadap penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* oleh pihak penyedia jasa di luar negeri tersebut antara lain risiko operasional, hukum dan reputasi serta analisis *country risk*.

^{*)} Realisasi rencana Bank yang telah disetujui oleh Bank Indonesia untuk menggunakan pihak penyedia jasa dalam menyelenggarakan *data center* dan DRC di luar negeri dilaporkan 1 bulan setelah penyelenggaraan TI tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI.



Lampiran 2.3.4

**REALISASI PENYELENGGARAAN
PEMROSESAN TRANSAKSI BERBASIS TEKNOLOGI INFORMASI
OLEH PIHAK LAIN DI DALAM NEGERI ^{*)}**

1. Aktivitas dan produk yang penyelenggaraannya yang diserahkan kepada pihak penyedia jasa termasuk uraian atau penjelasan dan flow chart dari prosedur pelaksanaan (SOP).
2. Lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....
 - c. Pemrosesan transaksi.....
3. Lampirkan *copy* perjanjian antara bank dan pihak penyedia jasa penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di dalam negeri.
4. Lampirkan hasil pengujian/*testing* atas penggunaan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di dalam negeri tersebut.
5. Lampirkan Berita Acara pengalihan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di dalam negeri.
6. Lampirkan hasil *post implementation review* (PIR) atas penggunaan pihak penyedia jasa dalam menyelenggarakan Pemrosesan Transaksi Berbasis Teknologi Informasi di dalam negeri yang antara lain mencakup review mengenai:
 - a. system berjalan dengan baik (*system performance review*);
 - b. kesesuaian dengan user requirement;
 - c. problem yang terjadi dan solusi/eskalasi/penyelesaian yang dibuat;
 - d. efektifitas pengamanan yang ditetapkan.
7. Lampirkan gambar garis pelaporan dan informasi setelah pemrosesan transaksi diserahkan kepada pihak penyedia jasa.
8. Lampirkan hasil analisis atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya *confidentiality, integrity, availability* dan *authentication* dalam penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi yang diserahkan kepada pihak penyedia jasa di luar negeri.
9. Lampirkan analisis risiko terkini oleh Bank terhadap penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak penyedia jasa antara lain risiko operasional, hukum dan reputasi.

*) Realisasi rencana Bank untuk menggunakan pihak penyedia jasa dalam menyelenggarakan pemrosesan transaksi berbasis teknologi informasi di dalam negeri dilaporkan 1 (satu) bulan setelah penyelenggaraan pemrosesan transaksi berbasis teknologi informasi tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI.



Lampiran 2.3.5

**REALISASI PENYELENGGARAAN
PEMROSESAN TRANSAKSI BERBASIS TEKNOLOGI INFORMASI
OLEH PIHAK LAIN DI LUAR NEGERI ^{*)}**

1. Aktivitas dan produk yang penyelenggaraannya yang diserahkan kepada pihak penyedia jasa termasuk uraian atau penjelasan dan flow chart dari prosedur pelaksanaan (SOP).
2. Lokasi penyelenggaraan:
 - a. Pusat data (*data center*).....
 - b. *Disaster Recovery Center*.....
 - c. Pemrosesan transaksi
3. Lampirkan *copy* perjanjian antara bank dan pihak penyedia jasa penyelenggaraan pemrosesan transaksi berbasis teknologi informasi di luar negeri.
4. Lampirkan hasil pengujian/*testing* atas penggunaan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar negeri tersebut.
5. Lampirkan Berita Acara pengalihan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar negeri.
6. Lampirkan hasil *post implementation review* (PIR) atas penggunaan pihak penyedia jasa dalam menyelenggarakan pemrosesan transaksi berbasis teknologi informasi di luar negeri yang antara lain mencakup review mengenai:
 - a. system berjalan dengan baik (*system performance review*);
 - b. kesesuaian dengan user requirement;
 - c. problem yang terjadi dan solusi/eskalasi/penyelesaian yang dibuat;
 - d. efektifitas pengamanan yang ditetapkan.
7. Lampirkan gambar garis pelaporan dan informasi sekarang setelah penyelenggaraan diserahkan kepada pihak penyedia jasa.
8. Lampirkan hasil analisis atas pengendalian pengamanan yang digunakan untuk memastikan terpenuhinya *confidentiality, integrity, availability* dan *authentication* dalam penyelenggaraan pemrosesan transaksi berbasis teknologi informasi yang diserahkan kepada pihak penyedia jasa di luar negeri.
9. Lampirkan Surat Pernyataan dari pihak penyedia jasa TI sebagai pihak terafiliasi tidak keberatan bila Bank Indonesia hendak memeriksa penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi.

^{*)} Realisasi rencana Bank untuk menggunakan pihak penyedia jasa dalam menyelenggarakan pemrosesan transaksi berbasis teknologi informasi di luar negeri dilaporkan 1 (satu) bulan setelah penyelenggaraan pemrosesan transaksi berbasis teknologi informasi tersebut efektif dioperasikan sebagaimana dipersyaratkan pada PBI.



Lampiran 2-4

**LAPORAN TAHUNAN PENGGUNAAN
TEKNOLOGI INFORMASI^{*)}**

Nama Bank Alamat Kantor Pusat Bank No. Telp.
Nama Pelapor Kantor/Divisi/Bagian Pelapor Alamat Pelapor No. Telp.
Tanggal Laporan _ _ _ _ _

1. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan Manajemen pada Lampiran 2.1.1?

	Ada	Tidak Ada	
--	-----	-----------	--

Bila ada, apakah perubahan tersebut sudah dilaporkan kepada Bank Indonesia?

	Sudah	Belum	
--	-------	-------	--

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

2. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan Aplikasi dan Pengembangan (*Development & Acquisition*) pada Lampiran 2.1.2?

	Ada	Tidak Ada	
--	-----	-----------	--

Bila ada, apakah perubahan tersebut sudah dilaporkan kepada Bank Indonesia?

	Sudah	Belum	
--	-------	-------	--

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

*) Laporan disampaikan secara berkala selambat-lambatnya 1 (satu) bulan setelah akhir tahun pelaporan.

***) Format Lampiran laporan ini mengacu pada lembar terkait pada Laporan Penggunaan Teknologi Informasi atau format bebas sesuai bentuk materi atau hal yang akan dilaporkan oleh bank.



Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

Apakah terdapat perubahan yang signifikan pada aplikasi yang sudah operasional?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Jika ada perubahan yang signifikan tersebut, lampirkan data nama aplikasi, keterangan perubahan yang dilakukan, tempat dan tanggal implementasi.

3. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan Operasional TI pada Lampiran 2.1.3?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, apakah perubahan tersebut sudah dilaporkan kepada Bank Indonesia?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

4. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan Jaringan Komunikasi pada Lampiran 2.1.4?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, apakah perubahan tersebut sudah dilaporkan kepada Bank Indonesia?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

5. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan Pengamanan Informasi pada Lampiran 2.1.5?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, apakah perubahan tersebut sudah dilaporkan kepada Bank Indonesia?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

6. Terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan *Business Continuity Plan* pada Lampiran 2.1.6 ?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

***) Format Lampiran laporan ini mengacu pada lembar terkait pada Laporan Penggunaan Teknologi Informasi atau format bebas sesuai bentuk materi atau hal yang akan dilaporkan oleh bank.



Bila ada, apakah perubahan tersebut sudah dilaporkan ke BI?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

7. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan penggunaan komputer Mikro pada Pengguna pada Lampiran 2.1.7?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, apakah perubahan tersebut sudah dilaporkan ke BI?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

8. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan *Electronic Banking* pada Lampiran 2.1.8 ?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

a. Jenis *Electronic Banking*:

1) *Electronic Banking* Transaksional

Apakah terdapat produk *Electronic Banking* baru yang bersifat transaksional?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Apakah rencana dan realisasi penerbitan produk di atas sudah dilaporkan ke BI?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Apakah terdapat perubahan fitur produk *Electronic Banking* yang bersifat transaksional namun tidak merupakan produk baru?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

2) *Electronic Banking* Non-Transaksional

Apakah terdapat produk baru atau perubahan pada *Electronic Banking* yang bersifat non-transaksional?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Apakah produk baru atau perubahan *Electronic Banking* yang bersifat non-transaksional namun meningkatkan risiko bank sudah dilaporkan ke BI?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------



b. Pelaporan untuk no.a.1 dan a.2.

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

9. Terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan fungsi Audit intern TI pada Lampiran 2.1.9 ?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, apakah perubahan tersebut sudah dilaporkan ke BI?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)

10. Apakah terdapat perubahan terhadap hal-hal yang telah dilaporkan dalam Laporan Penyelenggaraan TI oleh Pihak Lain pada Lampiran 2.1.10?

<input type="checkbox"/>	Ada	Tidak Ada	<input type="checkbox"/>
--------------------------	-----	-----------	--------------------------

Bila ada, apakah perubahan tersebut sudah dilaporkan ke BI?

<input type="checkbox"/>	Sudah	Belum	<input type="checkbox"/>
--------------------------	-------	-------	--------------------------

Bila sudah dilaporkan, sebutkan tanggal dan nomor surat.....

Bila belum dilaporkan, lampirkan data dan penjelasan mengenai perubahan tersebut.**)



Lampiran 2-5

LAPORAN KEJADIAN KRITIS, PENYALAHGUNAAN DAN/ATAU KEJAHATAN DALAM PENYELENGGARAAN TEKNOLOGI INFORMASI (TI)*)

Nama Bank ----- Alamat Kantor Pusat Bank ----- No. Telp. -----
Nama Pelapor ----- Kantor/Divisi/Bagian Pelapor ----- Alamat Pelapor ----- No. Telp. -----
Tanggal Laporan _ _ _ _ _

1. Tanggal kejadian
2. Kronologis dan evaluasi penyebab kejadian

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--
3. Terdapat unsur kesengajaan

	Ya	Tidak	
--	----	-------	--
4. Satuan kerja terkait termasuk orang yang dapat dihubungi lebih lanjut
5. Dampak/akibat yang ditimbulkan (berilah tanda "X" pada kotak yang sesuai)
 - a. Kerugian keuangan

	Ya	Tidak	
--	----	-------	--
 - b. Gangguan operasional

	Ya	Tidak	
--	----	-------	--

Jika jawaban "Ya", lampirkan bentuk gangguan operasional yang terjadi dan contingency plan yang telah diterapkan.
 - c. Tidak terjaminnya kerahasiaan dan integritas data

	Ya	Tidak	
--	----	-------	--

Jika jawaban "Ya", lampirkan bentuk ancaman terhadap kerahasiaan dan integritas data.
6. Rencana tindak lanjut bank

	Terlampir	Tidak Terlampir	
--	-----------	-----------------	--

*) Kejadian kritis yang dimaksud adalah kejadian yang menambah exposure risiko secara signifikan. Penyalahgunaan/kejahatan dalam penyelenggaraan Teknologi Informasi adalah tindakan yang mengakibatkan timbulnya kerugian keuangan dan atau mengganggu kelancaran operasional bank.



Lampiran 2.6

**PERMOHONAN PERSETUJUAN ULANG PENYELENGGARAAN
DATA CENTER DAN ATAU DISASTER RECOVERY CENTER OLEH
PIHAK LAIN DI LUAR NEGERI BAGI
KANTOR CABANG BANK ASING^{*)}**

1. Lokasi penyelenggaraan:
 - a. Pusat data (*Data Center*).....
 - b. *Disaster Recovery Center*.....

Lampirkan data nama dan alamat serta kepemilikan penyelenggara *Data Center* dan atau *Disaster Recovery Center*.
2. Lampirkan perjanjian antar bank dengan penyelenggara *Data Center* dan atau *Disaster Recovery Center* di luar negeri yang telah disesuaikan dengan persyaratan dalam Peraturan Bank Indonesia.
3. Lampirkan gambar *IT Architecture* yang mencakup *Data Center* dan atau *Disaster Recovery Center* yang diserahkan kepada pihak penyedia jasa.
4. Lampirkan Surat Pernyataan dari Bank mengenai kesediaan Bank memberikan akses kepada auditor intern, ekstern maupun Bank Indonesia untuk memperoleh data dan informasi secara tepat waktu setiap kali dibutuhkan.
5. Lampirkan :
 - a. Surat Pernyataan dari otoritas pengawas setempat dalam hal pihak penyedia jasa TI merupakan cakupan pengawasan secara konsolidasi.
 - b. Surat Pernyataan tidak keberatan dari otoritas pengawas setempat bila Bank Indonesia hendak melakukan pemeriksaan penyelenggaraan pusat data (*Data Center*) dan atau *Disaster Recovery Center* tersebut.
 - c. Surat Pernyataan bahwa bank secara berkala akan menyampaikan hasil penilaian yang dilakukan kantor bank di luar negeri atas penerapan manajemen risiko pada pihak penyedia jasa. Surat Pernyataan ini mencantumkan periodisasi yang direncanakan.
 - d. Hasil penilaian oleh kantor Bank di luar negeri atas penerapan manajemen risiko yang dilakukan oleh pihak penyedia jasa.
6. Lampirkan rencana Bank mengenai:
 - a. peningkatan kualitas pelayanan kepada nasabah;
 - b. peningkatan kemampuan sumber daya manusia yang berkaitan dengan penyelenggaraan TI yang digunakan oleh Bank.

*) Bank yang sebelum dikeluarkannya ketentuan ini telah melaporkan kepada dan menerima surat tidak keberatan dari Bank Indonesia mengenai penyelenggaraan TI Bank yang diserahkan kepada pihak lain di luar negeri, wajib mengajukan permohonan persetujuan ulang kepada Bank Indonesia.