LAMPIRAN I

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 15 /SEOJK.03/2017

TENTANG

STANDAR PENYELENGGARAAN TEKNOLOGI INFORMASI BAGI BANK PERKREDITAN RAKYAT DAN BANK PEMBIAYAAN RAKYAT SYARIAH

PEDOMAN PENYELENGGARAAN TEKNOLOGI INFORMASI BAGI BANK PERKREDITAN RAKYAT DAN BANK PEMBIAYAAN RAKYAT SYARIAH

DAFTAR ISI

BAB I

WEWENANG DAN TANGGUNG JAWAB DIREKSI, DEWAN KOMISARIS, DAN SATUAN KERJA ATAU PEGAWAI YANG BERTANGGUNG JAWAB TERHADAP PENYELENGGARAAN TEKNOLOGI INFORMASI

Dalam penyelenggaraan Teknologi Informasi oleh BPR dan BPRS, Direksi dan Dewan Komisaris harus memastikan bahwa penyelenggaraan Teknologi Informasi telah berjalan sebagaimana mestinya dan sejalan dengan pencapaian visi dan misi BPR dan BPRS yang bersangkutan. Dalam rangka mewujudkan penyelenggaraan Teknologi Informasi yang efektif dan efisien, Direksi dan Dewan Komisaris harus melibatkan seluruh jenjang organisasi BPR dan BPRS.

Pengelolaan penyelenggaraan Teknologi Informasi oleh BPR dan BPRS secara efektif perlu dilakukan guna menghasilkan informasi yang diperlukan dalam pengambilan keputusan baik oleh BPR atau BPRS maupun pihak ekstern. Keberhasilan penyelenggaraan Teknologi Informasi BPR dan BPRS sangat tergantung pada komitmen Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi, maupun pengguna.

A. WEWENANG DAN TANGGUNG JAWAB DIREKSI

Wewenang dan tanggung jawab Direksi dalam penyelenggaraan Teknologi Informasi paling sedikit meliputi:

1. menetapkan rencana pengembangan dan pengadaan Teknologi Informasi BPR atau BPRS mencakup kegiatan:
   a) mengevaluasi, menyetujui, dan memantau proses pengembangan dan pengadaan Teknologi Informasi BPR atau BPRS; dan
   b) memastikan bahwa BPR dan BPRS memiliki perjanjian kerjasama dengan penyedia jasa Teknologi Informasi maupun penyedia Aplikasi Inti Perbankan yang mengatur peran, hubungan, hak, kewajiban, tanggung jawab dari semua pihak yang terikat dengan perjanjian kerjasama tersebut, serta memastikan bahwa perjanjian kerjasama tersebut memenuhi syarat sahnya perjanjian dan dapat

melindungi kepentingan BPR dan BPRS apabila timbul permasalahan di kemudian hari dalam hal BPR dan BPRS bekerjasama dengan penyedia jasa;

2. menetapkan kebijakan dan prosedur terkait penyelenggaraan Teknologi Informasi yang memadai dan mengomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna Teknologi Informasi;
3. memantau kecukupan kinerja dan upaya peningkatan penyelenggaraan Teknologi Informasi;
4. memastikan bahwa Teknologi Informasi yang digunakan BPR atau BPRS dapat mendukung perkembangan usaha, pencapaian tujuan bisnis, dan kelangsungan pelayanan terhadap nasabah BPR atau BPRS mencakup kegiatan:
   a) penyediaan data dan informasi yang akurat untuk mendukung sistem informasi manajemen BPR atau BPRS yang memadai;
   b) penyelenggaraan Teknologi Informasi BPR atau BPRS yang mampu mendukung perkembangan usaha BPR dan BPRS yang berkelanjutan;
   c) penyelenggaraan Teknologi Informasi BPR atau BPRS yang mampu mendukung kelangsungan pelayanan kepada nasabah BPR dan BPRS; dan
   d) memantau proses pengembangan dan pengadaan yang dilakukan oleh tim kerja sebagaimana dimaksud dalam Bab mengenai pengembangan dan pengadaan Sistem Elektronik.
5. memastikan terdapat peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan Teknologi Informasi diantaranya melalui pendidikan, pelatihan, atau sertifikasi yang memadai dan program edukasi untuk meningkatkan kesadaran atas pengamanan informasi;
6. memastikan tersedianya sistem pengelolaan pengamanan informasi (*information security management system*) yang efektif dan dikomunikasikan kepada satuan kerja penyelenggara dan pengguna Teknologi Informasi;
7. memastikan tersedianya kebijakan dan prosedur penyelenggaraan Teknologi Informasi yang memadai dan

dikomunikasikan serta diterapkan secara efektif baik pada satuan kerja yang bertanggung jawab terhadap penyelenggaraan maupun satuan kerja pengguna Teknologi Informasi paling sedikit meliputi kegiatan merumuskan kebijakan, rencana, dan anggaran penyelenggaraan Teknologi Informasi; dan

8. memastikan adanya dokumentasi terhadap setiap perubahan dan pengembangan yang dilakukan pada Sistem Elektronik termasuk perangkat lunak, baik yang dilakukan secara mandiri (*in-house*) maupun bekerjasama dengan penyedia jasa Teknologi Informasi.

B. WEWENANG DAN TANGGUNG JAWAB DEWAN KOMISARIS

Wewenang dan tanggung jawab Dewan Komisaris dalam penyelenggaraan Teknologi Informasi paling sedikit meliputi:

1. mengarahkan dan memantau rencana pengembangan dan pengadaan Teknologi Informasi BPR atau BPRS yang bersifat mendasar antara lain:
   a) perubahan secara signifikan terhadap konfigurasi Teknologi Informasi atau Aplikasi Inti Perbankan;
   b) pengadaan Aplikasi Inti Perbankan baru;
   c) kerja sama dengan penyedia jasa Teknologi Informasi; dan/atau
   d) pengembangan dan pengadaan Teknologi Informasi mendasar lainnya yang dapat menambah dan/atau meningkatkan risiko BPR atau BPRS; dan
2. mengevaluasi pertanggungjawaban Direksi terkait penyelenggaraan Teknologi Informasi BPR atau BPRS.

C. WEWENANG DAN TANGGUNG JAWAB SATUAN KERJA ATAU PEGAWAI YANG BERTANGGUNG JAWAB TERHADAP PENYELENGGARAAN TEKNOLOGI INFORMASI

Wewenang dan tanggung jawab satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi paling sedikit meliputi:

1. membantu Direksi dan Dewan Komisaris dalam penyelenggaraan Teknologi Informasi mencakup perencanaan, pelaksanaan dan pemantauan yang diwujudkan dalam kegiatan:
   a) memastikan kecukupan dan efektivitas kebijakan dan prosedur penyelenggaraan Teknologi Informasi;
   b) menerapkan seluruh kebijakan dan prosedur penyelenggaraan Teknologi Informasi yang telah ditetapkan oleh Direksi;
   c) memastikan terdapatnya pengawasan yang memadai dalam setiap pengembangan dan pengadaan sistem Teknologi Informasi;
   d) menyampaikan laporan penyelenggaraan Teknologi Informasi secara periodik kepada Direksi, dan jika diperlukan dapat mengusulkan tindakan untuk mengatasi kelemahan penyelenggaraan Teknologi Informasi yang ditemukan; dan
   e) memastikan tindakan yang tepat telah dilakukan untuk memperbaiki temuan audit baik dari auditor intern maupun auditor ekstern atau berdasarkan laporan pemeriksaan Otoritas Jasa Keuangan;
2. mendukung pengembangan dan pengadaan Teknologi Informasi paling sedikit mencakup:
   a) memastikan pengembangan dan pengadaan Teknologi Informasi BPR atau BPRS telah sesuai dengan kebijakan dan prosedur yang ditetapkan oleh Direksi;
   b) memastikan manajemen proyek terkait pengembangan dan pengadaan Teknologi Informasi dilaksanakan secara konsisten dan memadai; dan
   c) memastikan bahwa perjanjian tertulis antara BPR atau BPRS dengan penyedia aplikasi inti perbankan atau penyedia jasa penyelenggara Teknologi Informasi mencakup hal-hal yang telah diatur dalam POJK SPTI dan Surat Edaran Otoritas Jasa Keuangan ini;
3. mendukung implementasi, operasional, dan pemeliharaan Teknologi Informasi paling sedikit mencakup:

a) memberikan dukungan dalam penyelesaian permasalahan terkait Teknologi Informasi kepada satuan kerja pengguna secara responsif dan tepat waktu;

b) memastikan setiap informasi yang dimiliki oleh satuan kerja pengguna Teknologi Informasi mendapatkan perlindungan yang baik terhadap semua gangguan yang dapat menyebabkan kerugian akibat bocornya data/informasi penting; dan

c) memantau kinerja dari layanan Teknologi Informasi di BPR atau BPRS, antara lain persentase berapa lama sistem mati (*downtime error*), pelanggaran keamanan, perkembangan proyek, penerapan perjanjian tingkat layanan (*Service Level Agreement*/SLA).

4. melakukan upaya penyelesaian permasalahan terkait Teknologi Informasi, yang tidak dapat diselesaikan oleh satuan kerja pengguna secara efektif, efisien, dan tepat waktu; dan

5. melakukan dokumentasi terhadap setiap perubahan dan pengembangan yang dilakukan pada Sistem Elektronik termasuk perangkat lunak yang dilakukan secara mandiri (*in-house*) maupun bekerja sama dengan penyedia jasa Teknologi Informasi.

BAB II

PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK

Dalam rangka pengembangan dan pengadaan Sistem Elektronik yang dapat berupa pengembangan perangkat lunak secara intern, atau pembelian perangkat lunak, perangkat keras, dan/atau jasa pengembangan Sistem Elektronik dari penyedia jasa Teknologi Informasi, BPR dan BPRS wajib melakukan langkah-langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), serta mendukung pencapaian tujuan BPR atau BPRS, paling sedikit meliputi:

a. menetapkan dan menerapkan prosedur pengembangan dan pengadaan Sistem Elektronik secara konsisten;
b. menerapkan manajemen proyek dalam pengembangan dan pengadaan Sistem Elektronik;
c. melakukan *testing* yang memadai pada saat pengembangan dan pengadaan Sistem Elektronik, termasuk uji coba dengan melibatkan satuan kerja pengguna, untuk memastikan keakuratan dan berfungsinya Sistem Elektronik sesuai dengan kebutuhan pengguna serta kesesuaian suatu sistem dengan sistem yang lain;
d. melakukan dokumentasi terhadap pengadaan, pengembangan, dan pemeliharaan Sistem Elektronik;
e. memiliki manajemen perubahan Sistem Elektronik; dan
f. memastikan Sistem Elektronik BPR dan BPRS mampu menampilkan kembali informasi secara utuh.

Dalam rangka pengembangan dan pengadaan Sistem Elektronik, BPR dan BPRS harus menerapkan manajemen proyek untuk memastikan Sistem Elektronik telah dikembangkan dengan struktur yang baik dan telah mengakomodasi kebutuhan pengguna serta sesuai dengan Teknologi Informasi yang dimiliki BPR atau BPRS. Penerapan manajemen proyek dilakukan oleh suatu tim kerja yang memiliki anggota paling sedikit berasal dari satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi dan satuan kerja pengguna Teknologi Informasi. Tim kerja melaporkan setiap proses pengembangan dan pengadaan kepada Direksi.

Sementara satuan kerja audit intern atau pejabat eksekutif yang bertanggung jawab terhadap pelaksanaan fungsi audit intern merupakan pihak independen yang memberikan masukan bagi tim kerja dimaksud untuk memastikan kecukupan pengendalian dalam rangka pengembangan dan pengadaan Sistem Elektronik.

Dalam melaksanakan manajemen perubahan Sistem Elektronik selama dalam pengembangan aplikasi, seperti perubahan *user requirement*, perubahan teknologi pendukung yang digunakan, serta prosedur manajemen perubahan harus disusun, dilaksanakan, dan didokumentasikan dengan baik dan benar. 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 didokumentasikan dengan baik dan benar. Jejak audit (*audit trail*) dari semua perubahan yang diminta harus dipelihara.

A. KEBIJAKAN DAN PROSEDUR PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK

Hal-hal yang harus diperhatikan dalam kebijakan dan prosedur pengembangan dan pengadaan Sistem Elektronik paling sedikit meliputi:

1. setiap pengembangan dan pengadaan Sistem Elektronik harus selalu melibatkan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi;
2. terhadap Sistem Elektronik yang dikembangkan dan diadakan oleh penyedia jasa Teknologi Informasi, BPR dan BPRS harus melakukan proses pemilihan penyedia jasa Teknologi Informasi yang mengacu pada ketentuan mengenai pelaksanaan pekerjaan yang dialihdayakan sesuai ketentuan peraturan perundang-undangan. BPR dan BPRS harus juga memastikan kecukupan pelatihan dan petunjuk pelaksanaan (*manual book*) yang disusun sebagai bagian dari perjanjian kerjasama antara BPR atau BPRS dengan penyedia jasa Teknologi Informasi;
3. kebijakan serta prosedur pengembangan dan pengadaan Sistem Elektronik mengacu pada tahapan pengembangan, kesesuaian

spesifikasi dalam pengadaan, dan pelaksanaan aktivitas pemeliharaan;

4. kebijakan dan prosedur yang perlu dimiliki oleh BPR atau BPRS dalam manajemen proyek antara lain:
   a) analisis atas biaya dan manfaat mencakup analisis terhadap manfaat yang akan diterima dari Sistem Elektronik termasuk Aplikasi Inti Perbankan yang akan dikembangkan dan diadakan berdasarkan pada permasalahan dan kendala penyelenggaraan Sistem Elektronik termasuk Aplikasi Inti Perbankan saat ini dibandingkan dengan biaya yang harus dikeluarkan, termasuk untuk menentukan apakah akan menggunakan sumber daya intern atau alih daya;
   b) persyaratan pengamanan yang relevan sebelum Sistem Elektronik dikembangkan atau diadakan;
   c) pemisahan lingkungan (*environment*) untuk pengembangan, uji coba, dan operasional, termasuk pembatasan akses ke masing-masing lingkungan;
   d) analisis pemilihan perangkat lunak untuk memastikan terpenuhinya kebutuhan pengguna;
   e) perjanjian kerjasama antara BPR dan BPRS dengan penyedia jasa Teknologi Informasi yang memenuhi syarat sahnya perjanjian;
   f) penerapan manajemen pemeliharaan untuk semua proses pengembangan dan pengadaan Sistem Elektronik yang telah diimplementasikan;
   g) dokumentasi terhadap seluruh hasil pada setiap tahapan manajemen proyek; dan
   h) rencana proyek secara tertulis paling sedikit meliputi:
      1) identifikasi proyek dan manajer proyek;
      2) tujuan proyek, informasi latar belakang, dan strategi pengembangan dan pengadaan;
      3) deskripsi tanggung jawab utama dari tiap personel dalam manajemen proyek;
      4) prosedur untuk mengumpulkan dan menyebarkan informasi;

5) kriteria hasil yang ditargetkan untuk masing-masing tahap pengembangan dan pengadaan (*acceptance criteria*);
6) masalah keamanan dan pengendalian yang harus dipertimbangkan;
7) *cut off date* untuk mengalihkan penggunaan sistem aplikasi dari versi lama ke versi terbaru;
8) standar pengembangan dan pengadaan yang akan digunakan untuk pengawasan proyek, pengendalian sistem, dan kendali mutu (*quality assurance*);
9) pendokumentasian yang dihasilkan di setiap tahap proyek;
10) jadwal tahapan proyek dan aktivitas yang akan diselesaikan dalam tiap tahap;
11) estimasi anggaran dari keseluruhan biaya proyek;
12) rencana uji coba (*testing plan*) yang mengidentifikasi kebutuhan uji coba (*testing requirement*) dan jadwal prosedur uji coba; dan
13) rencana pelatihan yang mengidentifikasikan kebutuhan pelatihan dan jadwal agar pengguna dapat menggunakan dan memelihara aplikasi pasca implementasi;

5. prosedur manajemen perubahan Sistem Elektronik yang harus dibuat BPR atau BPRS adalah prosedur modifikasi yang paling sedikit mencakup:
   a) peninjauan ulang sebelum modifikasi dan otorisasi;
   b) pengujian sebelum modifikasi (dalam lingkungan pengujian yang terpisah);
   c) prosedur rekam cadang (*back up*) data sebelum modifikasi;
   d) dokumentasi yang terdiri atas:
      1) penjelasan modifikasi;
      2) alasan penerapan atau penolakan modifikasi yang diusulkan;
      3) nama individu yang melakukan modifikasi;
      4) tanggal dan waktu modifikasi dilakukan; dan
      5) salinan dari kode sumber (*source code*) yang diubah (jika ada).
   e) evaluasi setelah modifikasi;

6. dokumentasi yang harus dibuat selama proses modifikasi berlangsung terdiri atas:
   a) informasi yang menjadi prioritas;
   b) identifikasi sistem, Pangkalan Data (*Database*) dan satuan kerja yang terpengaruh;
   c) nama dari individu yang bertanggung jawab dalam membuat perubahan;
   d) kebutuhan sumber daya;
   e) prediksi biaya;
   f) prediksi tanggal penyelesaian;
   g) prediksi tanggal implementasi;
   h) pertimbangan potensi keamanan dan keandalan;
   i) kebutuhan uji coba;
   j) prosedur implementasi;
   k) perkiraan *downtime* pada saat implementasi;
   l) prosedur rekam cadang;
   m) pengkinian dokumentasi (rancangan aplikasi dan *scripts*, topologi jaringan, petunjuk pelaksanaan bagi pengguna, rencana kontinjensi, dan lain-lain);
   n) dokumentasi penerimaan modifikasi dari semua satuan kerja terkait (pengguna, teknologi, kendali mutu, keamanan, audit, dan lain-lain); dan
   o) dokumentasi audit pasca implementasi (perbandingan antara rencana dan hasil).

B. TAHAPAN PENGEMBANGAN SISTEM ELEKTRONIK

Salah satu bentuk metodologi yang dapat digunakan oleh BPR atau BPRS dalam melakukan pengembangan Sistem Elektronik adalah *System Development Life Cycle* (SDLC), yang terbagi menjadi tahapan inisiasi dan perencanaan, pendefinisian kebutuhan, desain, pemrograman, uji coba, implementasi, kaji ulang pasca implementasi, pemeliharaan, dan *disposal* dengan rincian sebagai berikut:

1. Tahap Inisiasi

   Inisiasi merupakan tahap perencanaan awal pengembangan Sistem Elektronik termasuk Aplikasi Inti Perbankan untuk

mendefinisikan lingkup, tujuan, jadwal dan anggaran awal yang diperlukan.

Tahap inisiasi diawali dengan identifikasi kebutuhan untuk menambahkan, menyempurnakan, atau memperbaiki suatu sistem melalui usulan tertulis untuk mendapatkan persetujuan Direksi. Pengajuan dilakukan oleh satuan kerja pengguna bersama dengan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.

Tahap inisiasi terdiri atas langkah-langkah paling sedikit sebagai berikut:

a) Pengajuan usulan tertulis yang berisi identifikasi kebutuhan pengguna untuk menambahkan, menyempurnakan, atau memperbaiki suatu sistem, tujuan, dan manfaat yang diharapkan, analisis biaya dan manfaat, serta manfaat dari Sistem Elektronik yang akan dikembangkan untuk mendukung strategi bisnis.

   Analisis atas biaya dan manfaat mencakup analisis terhadap manfaat yang akan diterima dari Sistem Elektronik termasuk Aplikasi Inti Perbankan yang akan dikembangkan dan diadakan berdasarkan pada permasalahan dan kendala penyelenggaraan Sistem Elektronik termasuk Aplikasi Inti Perbankan saat ini dibandingkan dengan biaya yang harus dikeluarkan, termasuk untuk menentukan apakah akan menggunakan sumber daya intern atau alih daya.

   Dari analisis tersebut BPR dan BPRS dapat menentukan alternatif yang akan digunakan. Dalam hal digunakan Sistem Elektronik dari penyedia jasa Teknologi Informasi, perlu pula diperhatikan kesesuaian spesifikasi dengan kebutuhan, pengaruh terhadap sistem yang telah ada, dukungan teknis purna jual, kondisi keuangan penyedia jasa Teknologi Informasi, kelengkapan dokumentasi, dan pelatihan.

b) Evaluasi Direksi terhadap usulan tertulis.

c) Persetujuan Direksi terhadap usulan tertulis mengenai pengembangan Sistem Elektronik baru atau perubahan Sistem Elektronik.

Setelah persetujuan pengembangan diperoleh pada tahap inisiasi, BPR dan BPRS 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 dilakukan pengkinian sesuai perkembangan proyek.

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

Pendefinisian Kebutuhan Pengguna (*User Requirement Definition*) adalah proses menganalisis kebutuhan pengguna terhadap Sistem Elektronik termasuk Aplikasi Inti Perbankan.

Berdasarkan usulan tertulis yang telah disetujui oleh Direksi, tim kerja dapat mulai menyusun *user requirement definition* secara detail sebagai dasar dimulainya pengembangan Sistem Elektronik. Pada tahap ini, seluruh kebutuhan pengguna Sistem Elektronik dikumpulkan berdasarkan contoh dokumen, spesifikasi proses dan sistem yang ada, wawancara dengan pengguna akhir dan riset serta analisis terhadap ketentuan yang berlaku.

Tahap pendefinisian kebutuhan pengguna ini terdiri atas:

a) Pengumpulan Kebutuhan (*Requirements Elicitation*) yang merupakan proses pengumpulan informasi mengenai tujuan pengembangan Sistem Elektronik, hasil yang diinginkan, kemampuan sistem dalam mengakomodasi kebutuhan bisnis proses dan cara penggunaan sistem.

b) Analisis Kebutuhan (*Requirements Analysis*) yang merupakan proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan. Pada tahap ini, ditentukan perkiraan umum dari waktu dan biaya pengembangan untuk tiap kebutuhan. Hasil analisis kebutuhan digunakan untuk menghasilkan

alur bisnis proses yang dapat memperjelas pemahaman mengenai kebutuhan dan solusi, baik bagi satuan kerja pengguna maupun pengembang perangkat lunak (satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi dalam hal pengembangan dilakukan secara mandiri, atau penyedia jasa Teknologi Informasi dalam hal pengembangan dilakukan melalui kerjasama).

c) Spesifikasi Kebutuhan (*Requirements Specification*) yang merupakan proses yang mendeskripsikan fungsional sistem yang akan dikembangkan, baik dari segi perangkat lunak maupun perangkat keras pendukung serta desain Pangkalan Data. Spesifikasi kebutuhan harus lengkap, komprehensif, dapat diuji, konsisten, jelas serta merinci kebutuhan *input*, proses, dan *output* yang dibutuhkan.

d) Pengelolaan Kebutuhan (*Requirements Management*) yang merupakan proses untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat proses pengembangan Sistem Elektronik.

3. Tahap Perancangan (Desain) Sistem Elektronik

Perancangan Sistem Elektronik merupakan proses konversi terhadap kebutuhan informasi, fungsi, dan jaringan terindentifikasi selama tahap inisiasi menjadi spesifikasi rancangan/desain yang akan digunakan pengembang.

Salah satu teknik desain adalah dengan menggunakan purwarupa (*prototype*) yang mengembangkan desain maket dari bagian Sistem Elektronik 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 dijadikan purwarupa dalam suatu proses iteratif (berulang-ulang) sampai disepakati desain yang akan digunakan. Organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi dan kendali mutu harus dilibatkan sebagai narasumber dalam proses evaluasi dan persetujuan terhadap desain yang akan digunakan.

Pada tahap desain diperlukan suatu standar pengendalian Sistem Elektronik yang mencakup kebijakan dan prosedur terkait dengan aktivitas pengguna dan pengendalian terintegrasi dalam Sistem Elektronik yang akan dikembangkan. Pada tahap ini, satuan kerja audit intern atau pejabat eksekutif yang bertanggung jawab terhadap pelaksanaan fungsi audit intern berpartisipasi memberikan masukan pengendalian yang harus diterapkan dalam Sistem Elektronik. Tahap ini diperlukan untuk meningkatkan keamanan, integritas dan keandalan 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 sedikit meliputi:

a) Pengendalian *Input*

Paling sedikit mencakup pemeriksaan terhadap validitas/kebenaran data, *range* data/parameter, dan duplikasi data yang di-*input*.

b) Pengendalian Proses

Memastikan proses bekerja secara akurat dan dapat menyimpan atau menolak informasi. Pengendalian proses yang dapat dilakukan secara otomatis oleh Sistem Elektronik paling sedikit mencakup *Error Reporting*, *Transaction Log*, pemeriksaan urutan, dan rekam cadang *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.

4. Tahap Pemrograman

Pemrograman merupakan proses konversi dari desain yang telah disetujui ke dalam bahasa pemrograman. Selama tahap ini, tim kerja harus membuat rencana uji coba yang harus dilakukan. Selain itu, tim kerja juga harus melakukan pengkinian rencana migrasi, implementasi dan pelatihan pengguna akhir, dan dokumentasi petunjuk pelaksanaan pemeliharaan.

Selanjutnya dalam tahap ini tim kerja harus memperhatikan:

a) Standar pemrograman, yang menjelaskan antara lain mengenai tanggung jawab *programmer*. Dalam rangka penerapan manajemen proyek, manajer proyek harus memahami secara keseluruhan mengenai proses pemrograman untuk memastikan tanggung jawab *programmer* telah sesuai, paling sedikit:
   1) Membatasi akses *programmer* terhadap data, aplikasi, utilitas, dan sistem di luar tanggung jawabnya. Pengendalian pengelolaan *library* dapat digunakan untuk mengelola akses tersebut; dan
   2) Pengendalian versi merupakan metode yang secara sistematis menyimpan kronologis dari salinan aplikasi yang disempurnakan serta menjadi salah satu dokumentasi aplikasi.

b) Dokumentasi
   1) Tim kerja harus mengelola dan memelihara dokumentasi yang detail untuk setiap aplikasi yang merupakan bagian dari Sistem Elektronik baik yang dikembangkan sendiri maupun yang dibeli atau dikembangkan oleh penyedia jasa Teknologi Informasi yaitu mencakup:
      a) deskripsi detail aplikasi;
      b) dokumentasi pemrograman;
      c) format yang digunakan (basis data, tampilan, dan informasi);
      d) standar penamaan; dan
      e) petunjuk pelaksanaan bagi pengguna akhir.
   2) Dokumentasi harus dapat mengidentifikasi standardisasi pengembangan, seperti narasi sistem, alur sistem, pengkodean khusus sistem, dan pengendalian intern dalam dokumen aplikasi itu sendiri.
   3) Dalam hal aplikasi dibeli atau dikembangkan oleh penyedia jasa Teknologi Informasi, tim kerja harus memastikan bahwa dokumentasi aplikasi dilakukan

sesuai dengan standar minimum dokumentasi BPR atau BPRS.

5. Tahap Uji Coba

Uji coba merupakan proses untuk menguji desain yang telah dikonversi menjadi bahasa pemrograman agar Sistem Elektronik termasuk Aplikasi Inti Perbankan berfungsi sesuai dengan kebutuhan pengguna serta hubungan dengan sistem aplikasi lain (*interoperability*) yang telah digunakan oleh BPR atau BPRS. Modifikasi yang dilakukan selama uji coba harus didokumentasikan untuk menjaga integritas keseluruhan dokumentasi aplikasi.

BPR dan BPRS harus melengkapi petunjuk pelaksanaan bagi satuan kerja pengguna dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi, serta menyiapkan rencana implementasi dan pelatihan. Uji coba yang dapat dilakukan oleh tim kerja, penyedia jasa Teknologi Informasi, atau penyedia Aplikasi Inti Perbankan yaitu:

a. *Unit Testing*

Unit testing merupakan uji coba atas fungsional setiap unit atau sub modul dari Sistem Elektronik termasuk Aplikasi Inti Perbankan yang telah selesai dikembangkan. *Unit testing* dilakukan sebelum *system integration testing* sehingga apabila terjadi sesuatu, konfigurasi/kode pada unit perangkat lunak tersebut dapat diubah tanpa menimbulkan kekhawatiran berdampak pada sistem lainnya.

b. *System Integration Testing*

System integration testing merupakan pengujian terhadap keseluruhan fungsional terhadap Sistem Elektronik termasuk Aplikasi Inti Perbankan setelah diintegrasikan menjadi satu kesatuan yang utuh. Pengujian ini dilakukan untuk menghindari kesulitan penelusuran jika terjadi *error* atau *bug* pada integrasi tersebut.

c. *Stress Testing*

Stress testing merupakan uji ketahanan terhadap kemampuan Sistem Elektronik atau Aplikasi Inti Perbankan dalam menangani proses atau transaksi dalam skala/jumlah yang besar.

Stress Testing dilakukan setelah tim kerja, penyedia jasa Teknologi Informasi, atau penyedia Aplikasi Inti Perbankan memberikan berita acara *system integration testing* kepada pengguna akhir.

d. *User Acceptance Test*

User Acceptance Test (UAT) merupakan proses uji coba akhir yang dilakukan oleh tim kerja, penyedia jasa Teknologi Informasi, atau penyedia Aplikasi Inti Perbankan dengan pengguna akhir terhadap Sistem Elektronik termasuk Aplikasi Inti Perbankan yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan. UAT hanya dapat dilakukan setelah tim kerja, penyedia jasa Teknologi Informasi, atau penyedia Aplikasi Inti Perbankan memberikan berita acara atas hasil pengujian *system integration testing.* Pada tahap ini, satuan kerja audit intern atau pejabat eksekutif yang bertanggung jawab terhadap pelaksanaan fungsi audit intern dapat ikut melakukan pengujian dengan tetap menjaga independensi guna meyakini ketersediaan, kecukupan, dan efektifitas pengendalian yang ada di sistem. Jika hasil UAT menunjukkan bahwa Sistem Elektronik termasuk Aplikasi Inti Perbankan telah sesuai dengan kebutuhan pengguna dan standar pengamanan BPR atau BPRS, harus dibuat suatu berita acara UAT yang disetujui pengguna akhir.

6. Tahap Implementasi

Tim kerja perlu melakukan hal-hal utama yaitu pemberitahuan jadwal implementasi, pelatihan pada pengguna, dan instalasi Sistem Elektronik termasuk Aplikasi Inti Perbankan yang telah

disetujui ke dalam lingkungan operasional. Hal-hal penting lainnya yang harus diperhatikan paling sedikit mencakup:

a. pemeriksaan integritas aplikasi berupa pengendalian yang memadai terhadap konversi dari kode sumber ke *object code* yang akan diimplementasikan;
b. migrasi data dari Sistem Elektronik lama ke Sistem Elektronik baru;
c. pemeriksaan akurasi dan keamanan data hasil migrasi pada sistem baru;
d. kemungkinan diberlakukannya *parallel run* antara sistem yang lama dengan yang baru, sampai dipastikan bahwa data pada sistem yang baru telah akurat dan andal;
e. integritas data, di mana BPR dan BPRS harus memastikan keakuratan, dan keandalan dari Pangkalan Data dan integritas data;
f. pada saat implementasi, BPR dan BPRS menghindari *patching data* karena dapat sangat mempengaruhi integritas data pada Pangkalan Data di peladen (*server*) operasional, untuk itu harus dihindari; dan
g. pengaturan penyimpanan kode sumber dan Pangkalan Data dari sistem lama.

7. Tahap Kaji Ulang Pasca Implementasi (*Post Implementation Review)*

Satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi harus melakukan kaji ulang pasca implementasi Sistem Elektronik untuk mengetahui bahwa seluruh aktivitas dalam rencana proyek telah dilaksanakan dan tujuan proyek telah tercapai.

Satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi harus menganalisis keefektifan aktivitas manajemen proyek dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek. Hasil analisis harus didokumentasikan dan dilaporkan kepada Direksi.

8. Tahap Pengoperasian

   Dalam pengoperasian Sistem Elektronik terdapat prosedur untuk pengawasan pelaksanaan pengoperasian, keamanan data, orisinalitas data, *inputing data*, dan pengaturan Pangkalan Data.

9. Tahap Pemeliharaan

   Pemeliharaan harus dilakukan terhadap perangkat keras, perangkat lunak, dan dokumentasi dalam rangka memastikan efektivitas operasional Sistem Elektronik. BPR dan BPRS harus menetapkan prosedur pemeliharaan yang sesuai dengan karakteristik dan risiko tiap proyek dari Sistem Elektronik yang ada.

10. Tahap *Disposal*

    Disposal merupakan proses terakhir dari pengembangan sistem termasuk data dengan cara menghapus atau menghancurkan sistem termasuk data. Setiap Sistem Elektronik hasil pengembangan dan pengadaan yang tidak digunakan dalam kegiatan operasional dan berdasarkan pertimbangan BPR atau BPRS diyakini tidak diperlukan dan tidak akan dipelihara lagi, akan memasuki tahap terakhir dalam SDLC yaitu tahap *disposal/termination*. Hal ini dilakukan untuk memastikan Sistem Elektronik yang digunakan dalam kegiatan operasional merupakan Sistem Elektronik yang paling akurat dan terkini, serta untuk menghindari penyalahgunaan oleh pihak yang tidak berwenang.

C. PENGADAAN SISTEM ELEKTRONIK

Dalam proses pengadaan Sistem Elektronik, untuk memastikan bahwa Sistem Elektronik yang diadakan telah memenuhi kebutuhan fungsional, kriteria keamanan, dan keandalan, BPR dan BPRS perlu memperhatikan hal-hal sebagai berikut:

1. Standar Pengadaan

   Standar pengadaan harus diterapkan untuk memastikan bahwa Sistem Elektronik yang diadakan memenuhi kebutuhan fungsional, kriteria keamanan, dan keandalan. Dalam

pengadaan Sistem Elektronik, BPR dan BPRS harus memperhatikan paling sedikit:

a. usulan tertulis rencana pengadaan Sistem Elektronik oleh tim kerja untuk mendapatkan persetujuan Direksi yang paling sedikit memuat analisis kebutuhan pengguna terhadap tujuan dan manfaat yang diharapkan, analisis biaya dan manfaat, serta manfaat dari Sistem Elektronik yang akan diadakan untuk mendukung strategi bisnis;
b. kesesuaian penyedia jasa Teknologi Informasi, perjanjian tertulis, lisensi, dan produk yang diperoleh terhadap kebutuhan penyelenggaraan Teknologi Informasi di BPR atau BPRS;
c. kesesuaian spesifikasi penawaran yang diajukan oleh penyedia jasa Teknologi Informasi dengan spesifikasi kebutuhan penyelenggaraan Teknologi Informasi di BPR atau BPRS;
d. perbandingan penawaran yang diajukan oleh penyedia jasa Teknologi Informasi satu dengan penyedia jasa Teknologi Informasi lainnya; dan
e. kondisi keuangan penyedia jasa Teknologi Informasi dan komitmen penyedia jasa Teknologi Informasi terhadap pelayanan.

2. Analisis Kebutuhan Pengguna

Analisis tentang kebutuhan pengguna merupakan hal yang perlu dilakukan sebelum dilaksanakannya evaluasi terhadap Sistem Elektronik yang akan diadakan. Dalam analisis ini perlu ditetapkan alasan untuk mengadakan Sistem Elektronik, kekurangan dari sistem yang digunakan saat ini, kebutuhan pengguna dan pemrosesan data, laporan yang dibutuhkan pengguna, keterkaitan Sistem Elektronik yang akan diadakan dengan sistem lainnya, serta sumber daya yang dibutuhkan untuk melakukan instalasi dan pemeliharaan Sistem Elektronik. Sistem Elektronik perlu ditelaah untuk memastikan tersedianya pengendalian pengamanan dan jejak audit, misalnya akses terhadap *file* data, proses otorisasi, pengendalian melalui *password*, catatan akses terhadap data, laporan tentang usaha

menembus pengamanan, dan kemampuan *program utilities* untuk mengubah data.

3. Analisis Biaya dan Manfaat

Dalam melakukan analisis biaya dan manfaat, tim kerja perlu melakukan perbandingan terhadap setiap alternatif penyedia jasa Teknologi Informasi mengenai biaya-biaya yang dibutuhkan, baik biaya langsung maupun tidak langsung. Kemampuan dan biaya dari setiap alternatif perlu dianalisis dan dibandingkan antara lain mencakup biaya yang ditawarkan dengan spesifikasi sesuai kebutuhan.

Perbandingan sebagaimana dimaksud di atas dapat dilakukan oleh tim kerja dengan cara mengumpulkan referensi dari pengguna lain atau informasi umum sebagai sumber informasi dalam mengevaluasi Sistem Elektronik yang akan diadakan, sistem komputer yang digunakan, perubahan atau modifikasi yang telah dilakukan setelah implementasinya, lama penggunaan, kualitas dukungan purna jual yang diberikan, kinerja pada Sistem Elektronik yang sama, dan informasi penting lainnya.

D. PEMELIHARAAN SISTEM ELEKTRONIK

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

1. Manajemen Perubahan

Direksi harus menetapkan SPO pengendalian perubahan secara

detail yang memuat prosedur otorisasi, uji coba, dokumentasi, implementasi, dan sosialisasi atas modifikasi teknologi tersebut. Modifikasi mencakup perangkat keras dan perangkat lunak. Modifikasi perangkat keras diperlukan untuk menggantikan peralatan yang lama, tidak berfungsi, atau untuk meningkatkan kinerja atau kapasitas penyimpanan. Modifikasi perangkat lunak dibutuhkan untuk memenuhi kebutuhan pengguna, memperbaiki permasalahan perangkat lunak, dan kelemahan pengamanan dalam penyelenggaraan Teknologi Informasi, atau mengimplementasikan teknologi baru. BPR dan BPRS harus mengoordinasikan modifikasi Sistem Elektronik melalui proses manajemen perubahan yang terpusat karena adanya keterkaitan antar Sistem Elektronik dan sistem operasional.

Berdasarkan tingkat kepentingannya, modifikasi digolongkan menjadi:

a. modifikasi utama (*major modification*), merupakan perubahan fungsional secara signifikan pada Sistem Elektronik yang antara lain disebabkan karena adanya konversi atau pengembangan sistem baru akibat adanya penggabungan, peleburan, atau perubahan kepemilikan BPR atau BPRS. Modifikasi utama harus diterapkan mengikuti proses yang terstruktur seperti yang dilakukan dalam tahapan pengembangan Sistem Elektronik;

b. modifikasi minor (*minor modification*), merupakan pelaksanaan perubahan pada Sistem Elektronik untuk meningkatkan kinerja, memperbaiki permasalahan, atau meningkatkan keamanan. Standar modifikasi minor harus mencakup permintaan perubahan, peninjauan kembali, dan prosedur persetujuan serta mensyaratkan BPR atau BPRS untuk merencanakan, menguji coba, dan mendokumentasikan semua perubahan sebelum dilakukan implementasi. BPR dan BPRS 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. BPR dan BPRS harus menetapkan standar persetujuan Sistem Elektronik yang mencakup

prosedur untuk memverifikasi hasil uji coba, memeriksa kode yang diubah, dan memastikan kesesuaian kode sumber. Setelah modifikasi Sistem Elektronik selesai, semua kode sumber harus diamankan dalam *library* baik versi terkini maupun versi sebelum diubah;

c. modifikasi darurat (*incidental modification*), dibutuhkan untuk memperbaiki permasalahan pada Sistem Elektronik atau mengembalikan proses operasional dengan cepat. Meskipun modifikasi tersebut harus diselesaikan dengan cepat, namun tetap harus diimplementasikan dan dikendalikan dengan baik. Modifikasi darurat juga harus diuji sebelum implementasi. Namun jika uji coba tidak dapat dilakukan secara menyeluruh pada modifikasi darurat sebelum implementasi, harus ada prosedur untuk melakukan rekam cadang (*backup*) *file* dengan benar. Hal ini penting agar BPR dan BPRS dapat membatalkan modifikasi jika modifikasi tersebut menyebabkan gangguan pada Sistem Elektronik.

1. *Patch Management*

   Penyedia jasa Teknologi Informasi mengembangkan dan mengeluarkan *patch* untuk memperbaiki permasalahan pada perangkat lunak, memperbaiki kinerja, dan meningkatkan keamanan. Jika terdapat *patch* baru, BPR dan BPRS harus mengevaluasi dampak secara teknis dari instalasi *patch* tersebut terhadap bisnis dan keamanan. BPR dan BPRS harus memiliki prosedur untuk mengidentifikasi ketersediaan *patch* dari sumber yang terpercaya. Standar pengaturan *patch* harus mencakup prosedur identifikasi, evaluasi, persetujuan, pengujian, instalasi, dan dokumentasi dari *patch*. BPR dan BPRS 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. *Library*

   Untuk memastikan ketersediaan aplikasi yang digunakan, BPR dan BPRS harus memiliki *Library* untuk menyimpan program. Selain itu perlu dilakukan penyimpanan atas informasi dan/atau

dokumen berupa data dan aplikasi yang berhubungan dengan peladen yang berasal dari pengembangan dan/atau pengujian. Penjelasan lebih lanjut mengenai *library* dimuat pada bab yang mengatur mengenai operasional Teknologi Informasi.

3. Konversi

   Dalam hal terjadi penggabungan, peleburan, atau perubahan kepemilikan BPR atau BPRS yang memerlukan pengintegrasian Sistem Elektronik, perlu dilakukan proses konversi. Dalam proses ini dilakukan modifikasi utama pada Sistem Elektronik yang ada dan pengembangan Sistem Elektronik baru apabila diperlukan. Dalam proses konversi ini, proses yang terstruktur seperti tahapan pengembangan Sistem Elektronik tetap harus diterapkan.

   Mengingat kompleksitas Sistem Elektronik di masing-masing BPR dan BPRS yang terlibat penggabungan, peleburan, atau perubahan kepemilikan, diperlukan analisis secara komprehensif terhadap dampak konversi pada kegiatan operasional BPR atau BPRS khususnya pemrosesan transaksi. Agar proses konversi berlangsung secara efektif, BPR dan BPRS perlu mengantisipasi peningkatan permintaan untuk *balancing, reconcilement, exception handling,* dukungan pengguna dan nasabah (*help desk*), penyelesaian masalah (*troubleshooting*), keterhubungan jaringan dan sistem administrasi.

4. Pemeliharaan Dokumentasi

   Standar dokumentasi harus mampu 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.

E. PERJANJIAN TERTULIS UNTUK PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK TERMASUK APLIKASI INTI PERBANKAN

Perjanjian tertulis dalam melakukan pengembangan dan pengadaan Sistem Elektronik termasuk Aplikasi Inti Perbankan paling sedikit mencakup:

1. cakupan pekerjaan/jasa;

2. biaya dan jangka waktu perjanjian kerja sama;
3. batasan risiko yang ditanggung oleh BPR atau BPRS dan penyedia jasa Teknologi Informasi (untuk pengembangan dan pengadaan Sistem Elektronik) atau penyedia Aplikasi Inti Perbankan (untuk pengembangan dan pengadaan Aplikasi Inti Perbankan) yang diakibatkan perubahan antara lain:
   a. ruang lingkup perjanjian kerja sama;
   b. ruang lingkup bisnis dan organisasi perusahaan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan; dan
   c. aspek hukum antara lain regulasi, hak cipta, paten, dan *trade mark*;
4. larangan bagi penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk menggunakan atau mengungkapkan informasi yang dimiliki BPR dan BPRS tanpa persetujuan BPR atau BPRS, termasuk dalam proses pelaksanaan *parallel run*;
5. jaminan dari penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk pengamanan dan kerahasiaan data terutama rahasia bank dan data pribadi nasabah termasuk bahwa Sistem Elektronik hanya bisa diakses oleh pemilik data (BPR dan BPRS) serta Sistem Elektronik tersebut tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam Sistem Elektronik dan data BPR atau BPRS;
6. tanggung jawab dari penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk menjaga keamanan dan kerahasiaan data/informasi BPR atau BPRS setelah berakhirnya perjanjian;
7. pernyataan bahwa penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan memberikan jaminan keandalan Sistem Elektronik, termasuk tidak menggunakan fitur Sistem Elektronik yang dapat mengakibatkan Sistem Elektronik tersebut tidak berfungsi dengan baik;
8. standar spesifikasi dan kinerja Sistem Elektronik paling sedikit mencakup:

a. kinerja dan fungsional yang diharapkan dari Sistem Elektronik;
b. persyaratan dan infrastruktur yang diperlukan untuk menjalankan Sistem Elektronik;
c. identifikasi kebutuhan uji coba guna menentukan pemenuhan standar kinerja Sistem Elektronik; dan
d. tindakan yang harus dilakukan penyedia jasa Teknologi Informasi apabila Sistem Elektronik gagal pada saat uji coba.

9. kesediaan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk memberikan dokumen teknis kepada BPR atau BPRS terkait dengan jasa yang dikerjakan oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan antara lain alur proses Teknologi Informasi, petunjuk pelaksanaan (*manual book*), struktur Pangkalan Data, dan aplikasi *online help* pada Sistem Elektronik yang bekerja secara interaktif;
10. jaminan ketersediaan akses ke kode sumber dalam hal:
    a. penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan tidak dapat memberikan layanan lagi;
    b. diperlukan modifikasi yang tidak dapat dilakukan oleh pihak penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan;
    c. perangkat lunak termasuk Aplikasi Inti Perbankan dibuat khusus untuk BPR atau BPRS (*propietary*); dan/atau
    d. perangkat lunak dinilai penting untuk kelangsungan operasional BPR atau BPRS.
11. kesediaan penyedia jasa Teknologi Informasi membantu proses konversi perangkat lunak termasuk data dan format data pada saat penggantian sistem diperlukan di masa mendatang;
12. penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan memberikan jaminan paling sedikit bahwa Sistem Elektronik:
    a. tidak melanggar hak kekayaan intelektual dari pihak lain;
    b. tidak mengandung kode rahasia atau pembatasan secara otomatis yang tidak diungkapkan pada perjanjian;

c. bekerja sesuai dengan spesifikasi dan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan bertanggung jawab dalam hal terjadi permasalahan; dan
d. dijamin pemeliharaannya oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan selama jangka waktu perjanjian.

13. *Service Level Agreement* (SLA) yang memuat standar kinerja dari penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan antara lain mengenai tingkat pelayanan yang diperjanjikan (*service levels*) dan target kinerja;
14. klausula bahwa SLA tetap berlaku dalam hal terjadi perubahan kepemilikan baik pada BPR atau BPRS maupun penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan;
15. laporan hasil pemantauan kinerja penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan yang terkait dengan SLA;
16. penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan tidak dapat memodifikasi Sistem Elektronik yang telah disepakati dalam perjanjian tanpa persetujuan dari kedua belah pihak;
17. keharusan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk melaporkan setiap kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam pengembangan dan pengadaan Sistem Elektronik termasuk Aplikasi Inti Perbankan yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelangsungan operasional BPR atau BPRS;
18. keharusan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk melakukan *transfer of knowledge* kepada BPR atau BPRS dengan merencanakan pelatihan terhadap sumber daya manusia BPR atau BPRS, antara lain mengenai jumlah sumber daya manusia yang dilatih, bentuk pelatihan, dan biaya yang diperlukan, yang bertujuan agar sumber daya manusia BPR atau BPRS memahami Teknologi Informasi yang digunakan terutama alur proses Teknologi Informasi dan struktur Pangkalan Data dari Sistem Elektronik

yang disediakan oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan tersebut;

19. sanksi dan/atau penalti terhadap pembatalan dan/atau pelanggaran perjanjian kerja sama;
20. kepatuhan pada ketentuan dan peraturan perundang-undangan termasuk penyelesaian sengketa dalam hal terjadi perselisihan;
21. pernyataan tidak keberatan dari penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan dalam hal Otoritas Jasa Keuangan atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-undangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan;
22. ketersediaan data dan informasi untuk keperluan pemeriksaan sebagaimana dimaksud pada angka 21, termasuk hak akses, baik secara *logic* maupun fisik terhadap data yang dikelola oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan;
23. pelaksanaan dan biaya dari pengkinian dan modifikasi Sistem Elektronik, dalam hal diperlukan;
24. keharusan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan untuk memiliki sumber daya manusia yang kompeten yaitu memiliki keahlian khusus di bidang Teknologi Informasi sebagaimana dibuktikan dengan sertifikat keahlian, surat keterangan pengalaman, dan/atau ijazah pendidikan sesuai dengan keperluan penyelenggaraan Teknologi Informasi;
25. keharusan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan:
    a. memastikan Aplikasi Inti Perbankan bekerja sesuai spesifikasi;
    b. bertanggung jawab dalam hal terjadi permasalahan pada Aplikasi Inti Perbankan;
    c. menjamin pemeliharaan Aplikasi Inti Perbankan, selama jangka waktu perjanjian.
26. BPR dan BPRS harus memastikan bahwa dalam klausula perjanjian kerja sama terdapat larangan melakukan subkontrak oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan kepada pihak ketiga tanpa persetujuan BPR atau

BPRS. Apabila terdapat kondisi dimana sebagian dari pengembangan perangkat harus disubkontrakkan, harus terdapat persetujuan tertulis dari BPR atau BPRS. Dalam memberikan persetujuan subkontrak dimaksud, BPR dan BPRS harus mempertimbangkan tingkat kesulitan dan ketersediaan ahli dalam pengembangan perangkat lunak tersebut serta keamanan data BPR atau BPRS. Disamping itu BPR dan BPRS harus memastikan terdapat klausula bahwa penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan bertanggung jawab terhadap perangkat lunak meskipun dirancang atau dikembangkan oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan lain;

27. standar spesifikasi pengembangan dan kinerja Sistem Elektronik paling sedikit terdiri atas:
    a. identifikasi dan spesifikasi fungsional di mana Sistem Elektronik operasional akan bekerja dan identifikasi *milestone* dari fungsional yang harus dipenuhi oleh penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan selama proses pengembangan dan pengadaan; dan
    b. pengaturan izin modifikasi dari spesifikasi dan standar kinerja selama proses pengembangan dan pengadaan;
28. informasi hak cipta (lisensi) perangkat lunak paling sedikit mencakup:
    a. bersifat eksklusif atau tidak ekslusif;
    b. siapa dan berapa banyak personil pada BPR dan BPRS yang dapat menggunakan perangkat lunak termasuk penggunaan dalam jaringan;
    c. jangka waktu lisensi penggunaan perangkat lunak;
    d. penggunaan perangkat lunak oleh entitas terkait lainnya terdapat dalam daftar lisensi;
    e. pemberlakuan atas salinan rekam cadang dari semua perangkat lunak penting yang dibutuhkan di tempat yang terpisah (*remote site*) dalam pelaksanaan rencana pemulihan bencana; dan
    f. tetap berlakunya lisensi dalam hal terjadi penggabungan, peleburan, atau perubahan pemilikan baik pada BPR dan

BPRS atau penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan.

29. ketentuan sebagaimana dimaksud pada angka 1 sampai dengan angka 28 berlaku *mutatis mutandis* bagi penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan yang menerima subkontrak.

BAB III

OPERASIONAL TEKNOLOGI INFORMASI

Bab ini membahas aktivitas dan pengendalian dari operasional Teknologi Informasi sebagai pedoman bagi BPR dan BPRS dalam rangka menerapkan standar penyelenggaraan Teknologi Informasi. Pengaturan atas operasional Teknologi Informasi yang memadai sangat penting untuk memastikan informasi pada sistem komputer adalah lengkap, akurat, kini, terjaga integritasnya, dan andal, serta terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan dan perusakan data.

Dalam penyelenggaraan Teknologi Informasi, BPR dan BPRS harus memastikan bahwa operasional Teknologi Informasi stabil, aman, dan efisien secara keseluruhan, baik yang diselenggarakan sendiri maupun bekerjasama dengan penyedia jasa Teknologi Informasi. BPR dan BPRS harus menetapkan kebijakan dan prosedur operasional Teknologi Informasi yang menjamin kesinambungan operasional Teknologi Informasi dan memastikan penerapannya baik pada satuan kerja pengguna, satuan kerja penyelenggara atau penyedia jasa Teknologi Informasi. Operasional Teknologi Informasi 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. Demikian juga dengan pemrosesan, dapat dilakukan di berbagai lokasi yang berjauhan namun saling terkait, baik secara *online*, *realtime*, maupun *offline*.

A. KEBIJAKAN DAN PROSEDUR OPERASIONAL TEKNOLOGI INFORMASI

BPR dan BPRS wajib memiliki kebijakan dan prosedur yang mencakup setiap aspek operasional Teknologi Informasi sesuai dengan POJK SPTI. Kedalaman dan cakupan kebijakan dan prosedur tersebut disesuaikan dengan kompleksitas operasional BPR dan BPRS. Kebijakan dan prosedur harus dijabarkan secara tertulis yang digunakan dalam pelaksanaan operasional Teknologi Informasi. Kebijakan dan prosedur memuat rincian tugas, tanggung jawab, pemberian wewenang, dan pedoman pelaksanaan bagi satuan kerja pengguna dan satuan kerja penyelenggara Teknologi Informasi. Selain

itu, BPR dan BPRS harus menetapkan persyaratan yang harus dipenuhi terkait perangkat keras dan perangkat lunak yang digunakan di lingkungan produksi, pengujian, dan pengembangan dalam penyelenggaraan Teknologi Informasi BPR dan BPRS.

1. Kebijakan dan Prosedur Pengelolaan Data

   BPR dan BPRS harus menjalankan kebijakan dan prosedur pengelolaan data atas penyelenggaraan Teknologi Informasi yang mencakup:

   a) Kebijakan dan Prosedur Operasional Pusat Data

      Kebijakan dan prosedur yang diterapkan dalam aktivitas operasional Pusat Data mencakup aktivitas menjalankan tugas rutin maupun non-rutin. Aktivitas yang terkait dengan operasional Pusat Data paling sedikit:

      (1) penjadwalan tugas

          BPR dan BPRS harus memiliki dan melaksanakan jadwal semua tugas yang harus dijalankan di Pusat Data operasional Teknologi Informasi secara efektif dan aman;

      (2) pengoperasian tugas

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

      (3) pendistribusian laporan/*output*

          Hasil informasi yang diproduksi oleh sistem (*output*), dalam bentuk *softcopy* atau *hardcopy*, dapat merupakan informasi yang sensitif atau rahasia. BPR dan BPRS harus memiliki prosedur pendistribusian laporan/*output* yang meliputi penentuan informasi yang akan dihasilkan baik informasi umum atau rahasia, pendistribusian *output* baik secara *hardcopy* maupun *softcopy,* dan pemusnahan *output* yang sudah tidak diperlukan lagi. Prosedur tersebut diperlukan untuk menghindari terbukanya informasi yang bersifat rahasia, meningkatnya biaya akibat adanya *output*

yang tidak diperlukan, dan memastikan keamanan *output*;

(4) proses rekam cadang baik *on-site* maupun *off-site, restore,* unduh (*download),* dan unggah (*upload*) untuk data/Pangkalan Data; dan/atau

(5) pengaktifan jejak audit.

b) Kebijakan dan Prosedur Pengelolaan Pangkalan Data (*Database*)

Kegagalan dalam mengelola dan mengamankan Pangkalan Data dapat mengakibatkan perubahan, pemusnahan, atau pengungkapan informasi yang bersifat rahasia baik oleh pengguna secara sengaja maupun tidak sengaja ataupun oleh pihak lain yang tidak berhak. Pengungkapan informasi rahasia oleh pihak yang tidak berwenang dapat mengakibatkan risiko reputasi, operasional dan dapat menyebabkan kerugian finansial. BPR dan BPRS harus membuat kategori jenis data pada Pangkalan Data yang termasuk dalam kategori informasi umum atau informasi rahasia. Pangkalan Data yang menyimpan informasi rahasia membutuhkan pengendalian yang lebih ketat dibandingkan Pangkalan Data yang menyimpan informasi yang bersifat umum. Untuk itu, BPR dan BPRS harus memiliki fungsi *Database Administrator* (DBA) yang bertanggung jawab terhadap pengelolaan Pangkalan Data BPR atau BPRS.

Kebijakan dan prosedur yang harus dimiliki BPR dan BPRS terkait Pangkalan Data adalah pengaksesan, pemeliharaan, penanganan permasalahan dan administrasi Pangkalan Data. Bagi BPR dan BPRS yang memiliki *Data Warehouse* (DWH), BPR dan BPRS harus menerapkan prosedur yang sama dengan kebijakan dan prosedur pengelolaan Pangkalan Data.

c) Kebijakan dan Prosedur Pengelolaan *Library*

Library merupakan kumpulan perangkat lunak atau data yang memiliki fungsi tertentu dan disimpan serta siap untuk digunakan. Dalam rangka pengelolaan *library,* BPR dan BPRS harus melakukan inventarisasi dan menyimpan

seluruh perangkat lunak dan data yang tersimpan dalam berbagai media, antara lain *tape* dan *disc*, termasuk salinan dari seluruh kebijakan dan prosedur seperti petunjuk pelaksanaan aplikasi di Pusat Data.

BPR dan BPRS harus memiliki kebijakan dan prosedur terkait pengelolaan *library* yang antara lain meliputi prosedur pengamanan akses data, penanganan media penyimpan data (untuk data/ Pangkalan Data dan jejak audit, masa retensi dan pengujian media penyimpan data, serta *log* akses terhadap media penyimpanan data).

Dalam membuat kebijakan dan prosedur serta standar untuk *library*, BPR dan BPRS harus memperhatikan kecukupan prosedur penyimpanan (*storage*)/rekam cadang dan pemusnahan (*disposal*) media. BPR dan BPRS harus selalu melakukan pengkinian rekam cadang data dan aplikasi untuk memastikan rekam cadang dimaksud dapat digunakan dalam rangka memulihkan sistem, aplikasi, dan data pada saat terjadi bencana atau gangguan lainnya.

2. Kebijakan dan Prosedur Perencanaan, Pengelolaan, Pemeliharaan, dan Penghapusan Perangkat Keras dan Perangkat Lunak

BPR dan BPRS harus memiliki kebijakan dan prosedur untuk operasional Teknologi Informasi yang terkait dengan perangkat keras maupun perangkat lunak meliputi:

a) Kebijakan dan Prosedur Perencanaan Kapasitas

BPR dan BPRS harus memiliki kebijakan dan prosedur perencanaan kapasitas untuk dapat memastikan bahwa perangkat keras dan perangkat lunak yang digunakan BPR atau BPRS telah sesuai dengan kebutuhan operasional bisnis dan mengantisipasi perkembangan usaha BPR atau BPRS. Tanpa perencanaan kapasitas yang baik, BPR dan BPRS menghadapi risiko kekurangan atau pemborosan sumber daya Teknologi Informasi. Perencanaan kapasitas disusun secara berkala dan selalu dilakukan pengkinian untuk mengakomodasi perubahan yang ada.

b) Kebijakan dan Prosedur Pengelolaan Konfigurasi Perangkat Keras dan Perangkat Lunak

Dalam pengelolaan konfigurasi perangkat keras dan perangkat lunak, BPR dan BPRS harus menetapkan prosedur terkait:

(1) proses instalasi perangkat keras dan perangkat lunak;

(2) pengaturan parameter (*hardening*) perangkat keras dan perangkat lunak; dan

(3) inventarisasi dan pengkinian informasi perangkat keras, perangkat lunak, perangkat jaringan, media penyimpan, dan perangkat pendukung lainnya yang terdapat di Pusat Data.

Inventarisasi yang dilakukan meliputi:

(a) perangkat keras

inventarisasi perangkat keras harus dilakukan secara menyeluruh termasuk inventarisasi terhadap perangkat keras yang dimiliki oleh pihak lain tetapi berada di BPR atau BPRS. Informasi perangkat keras yang penting untuk dilakukan pengkinian antara lain nama penyedia jasa Teknologi Informasi, model perangkat keras, tanggal pembelian dan instalasi, kapasitas *processor*, memori utama, kapasitas penyimpanan, sistem operasi, fungsi, dan lokasi.

(b) perangkat lunak

BPR dan BPRS harus melakukan inventarisasi atas informasi mengenai nama dan jenis perangkat lunak (sistem operasi, sistem aplikasi, atau sistem utilitas). Informasi lain yang harus ada di dalam inventarisasi perangkat lunak meliputi nama pembuat atau penyedia jasa Teknologi Informasi, 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 pengguna (*user*).

(c) perangkat jaringan

infrastruktur jaringan merupakan hal yang penting bagi operasional BPR atau BPRS, sehingga satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi harus mendokumentasikan konfigurasi jaringan secara lengkap. Informasi dalam hasil dokumentasi mencakup antara lain:

i. diagram jaringan;
ii. identifikasi seluruh koneksi intern dan ekstern BPR atau BPRS;
iii. daftar dan kapasitas peralatan jaringan seperti *switch, router, hub, gateway, firewall*, dan lain-lain;
iv. identifikasi penyedia jasa Teknologi Informasi terkait telekomunikasi di intern BPR atau BPRS, antara BPR atau BPRS dengan pihak lain, dan dengan internet;
v. rencana perluasan dan perubahan konfigurasi jaringan; dan
vi. 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 rekam cadang.

(e) perangkat pendukung Pusat Data

BPR dan BPRS harus menginventarisasi perangkat pendukung Pusat Data antara lain *Uninterruptible Power Supply* (UPS) dan *power control*, pendeteksi dan pemadam api (*fire detection and extinguisher*), pendingin udara (*air*

conditioning), serta pengukur suhu dan kelembaban udara.

c) Kebijakan dan Prosedur Pemeliharaan Perangkat Keras dan Perangkat Lunak

(1) Perawatan Perangkat Keras dan Fasilitas Pusat Data

Perawatan preventif secara berkala terhadap peralatan Teknologi Informasi perlu dilakukan untuk meminimalkan kegagalan pengoperasian peralatan tersebut dan untuk mendeteksi secara dini permasalahan yang potensial. Untuk itu BPR dan BPRS perlu memiliki kontrak perawatan dengan penyedia jasa Teknologi Informasi guna memastikan ketersediaan dukungan perawatan dari penyedia jasa Teknologi Informasi. Semua perawatan yang dilakukan hendaknya didasarkan jadwal yang telah ditetapkan, didokumentasikan pada suatu *log* dan dilakukan evaluasi secara berkala.

(2) Pengamanan Fisik dan Pengendalian Lingkungan Pusat Data

(a) Pengendalian Akses Fisik Pusat Data

Akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik. Pintu Pusat Data harus selalu terkunci, apabila perlu bisa dilengkapi dengan kartu akses dan/atau *biometric device.* Ruang Pusat Data tidak boleh diberi label atau papan petunjuk (*signing board*) sehingga orang mudah mengenalinya. BPR dan BPRS harus memiliki *logbook* untuk mencatat tamu yang memasuki Pusat Data.

(b) Pengendalian lingkungan Pusat Data

Dalam rangka penerapan pengendalian lingkungan Pusat Data, satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi harus melakukan paling sedikit:

i. mengawasi dan memantau lingkungan Pusat Data, antara lain mencakup: sumber listrik, api, air, suhu, kelembaban udara. Pengendalian lingkungan yang dapat diterapkan antara lain: penggunaan UPS, *raised floor* (lantai yang ditinggikan), pengaturan suhu dan kelembaban udara (AC, termometer, dan hidrometer), pendeteksi asap/api/panas, sistem pemadaman api, kamera CCTV (*Closed Circuit Television*), dan pengendali hama (*pest control*).

ii. 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, BPR dan BPRS perlu memastikan pengatur voltase listrik, UPS dan generator listrik dapat bekerja dengan baik pada saat diperlukan. BPR dan BPRS sebaiknya menggunakan metode pemindahan secara otomatis (*automatic switching*) jika terjadi gangguan pada salah satu sumber listrik untuk menjaga pasokan listrik yang sesuai dengan kebutuhan peralatan.

iii. memastikan Pusat Data memiliki alat pendeteksi api dan asap serta pipa pembuangan air. Selanjutnya, BPR dan BPRS 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 Pusat Data.

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

(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 peladen tetap dalam keadaan menyala, kapasitas Pangkalan Data dan utilitas peladen tidak melampaui limit, dan fasilitas pendukung berfungsi dengan baik.

d) Kebijakan dan Prosedur Penghapusan Perangkat Keras dan Perangkat Lunak (*Disposal*)

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

1) memindahkan data dari sistem operasional ke media rekam cadang dengan mekanisme sesuai prosedur, termasuk prosedur uji coba dan rekam cadang;
2) menyimpan dokumentasi sistem sebagai persiapan jika diperlukan untuk meng-*install* ulang suatu sistem ke peladen operasional;
3) mengelola arsip data sesuai masa retensi; dan
4) menghancurkan data yang habis masa retensinya.

3. Kebijakan dan Prosedur Pengelolaan Perubahan (*Change Management*)

Change Management adalah prosedur yang mengatur penambahan, penggantian, maupun penghapusan objek di

lingkungan produksi. Objek dimaksud dapat berupa data, aplikasi, menu, perangkat komputer, perangkat jaringan, dan proses. BPR dan BPRS harus memiliki kebijakan dan prosedur *Change Management* yang paling sedikit mencakup permintaan, analisis, dan persetujuan perubahan, serta instalasi perubahan termasuk pemindahan perangkat keras dan perangkat lunak dari lingkungan pengujian ke lingkungan operasional.

Change Management harus memperhatikan hal-hal sebagai berikut:

a) Pengendalian Perubahan

Ketergantungan antar Sistem Elektronik yang digunakan pada berbagai satuan kerja memerlukan penyelenggaraan Teknologi Informasi yang terintegrasi. Oleh karena itu semua perubahan harus melalui fungsi pengawasan dalam *Change Management* yang terkoordinasi dan melibatkan perwakilan dari satuan kerja bisnis, satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi, keamanan informasi, dan audit intern. Prosedur instalasi perubahan harus memperhatikan kelangsungan operasional pada lingkungan produksi, pengawasan, dan pengaturan pengamanan penyelenggaraan Teknologi Informasi. Standar minimum yang diatur harus mencakup risiko, pengujian, otorisasi dan persetujuan, waktu implementasi, validasi setelah proses *install*, dan pemulihan (*recovery).*

b) *Patch Management*

Dalam *Change Management*, BPR dan BPRS harus memiliki dokumentasi yang lengkap tentang instalasi *patch* yang dilakukan. Selain itu BPR dan BPRS harus memastikan bahwa BPR atau BPRS menggunakan versi perangkat lunak terbaru yang paling sesuai. BPR dan BPRS 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 Elektronik BPR atau BPRS, atau terjadi penggabungan data dari beberapa Sistem Elektronik yang berbeda. Dalam hal terdapat migrasi data, BPR dan BPRS perlu memiliki kebijakan dan 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, rekam cadang, manajemen penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan (vendor), dan *post implementation review.*

4. Kebijakan dan Prosedur Penanganan Kejadian/Permasalahan

Prosedur penanganan kejadian/permasalahan harus mencakup perangkat keras, sistem operasi, sistem aplikasi, perangkat jaringan, dan peralatan keamanan.

BPR dan BPRS harus memelihara sarana yang diperlukan untuk menangani permasalahan antara lain:

a) *Help desk*

BPR dan BPRS harus memiliki fungsi *help desk* agar permasalahan yang dihadapi oleh pengguna dapat segera ditangani.

Hal-hal yang perlu diperhatikan dalam fungsi *help desk,* yaitu:

1) Tersedianya dokumentasi permasalahan yang lengkap yaitu dokumentasi permasalahan harus mencakup data pengguna, penjelasan masalah, dampak pada sistem (*platform*, aplikasi atau lainnya), kode prioritas, status resolusi saat ini, pihak yang bertanggung jawab terhadap resolusi, akar permasalahan (jika teridentifikasi), target waktu resolusi, dan *field* komentar untuk mencatat kontak pengguna dan informasi relevan lainnya.
2) BPR dan BPRS perlu menggunakan sistem yang berbasis pengetahuan untuk memberikan dukungan kepada staf *help desk* tentang alternatif solusi

permasalahan yang umum terjadi. BPR dan BPRS secara berkala melakukan pengkinian terhadap sistem tersebut dengan informasi yang didapat dari penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan dan dari pengalaman staf *help desk*.

b) Penanganan Penggunaan *Super User*

Super user adalah *user-id* yang memiliki kewenangan sangat luas. Dalam rangka penanganan permasalahan, BPR dan BPRS harus menetapkan prosedur penanganan *super user* agar penggunaannya tidak disalahgunakan. Prosedur tersebut paling sedikit mengatur hal-hal sebagai berikut:

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

5. Kebijakan dan Prosedur Pengendalian Pertukaran Informasi (*Exchange of Information*)

Pengiriman informasi secara *online* maupun melalui media penyimpan harus dikelola secara memadai oleh BPR dan BPRS untuk mencegah risiko terkait pengamanan informasi. BPR dan BPRS harus memiliki prosedur pengelolaan transmisi informasi secara fisik dan *logic* paling sedikit:

a. permintaan dan pemberian informasi oleh pihak intern dan ekstern; dan
b. pengiriman informasi melalui berbagai media, seperti: *hardcopy*, *disc*, surat elektronik, pos, dan internet.

Pada BPR dan BPRS skala besar dengan kompleksitas Teknologi Informasi yang tinggi, BPR dan BPRS harus mempertimbangkan pemisahan segmen WAN (*Wide Area Network*) dan LAN (*Local Area Network*) dengan perangkat pengamanan (seperti *firewall*) yang membatasi akses dan lalu lintas keluar masuknya data.

6. Kebijakan dan Prosedur Fungsi Kendali Mutu (*Quality Assurance)*

   BPR dan BPRS perlu mempertimbangkan untuk memiliki fungsi kendali mutu dalam memahami proses bisnis BPR atau BPRS. Fungsi kendali mutu melakukan penilaian kualitas perangkat keras dan perangkat lunak sesuai dengan standar yang ditetapkan. Setiap pembuatan dan perubahan sistem harus melalui persetujuan fungsi kendali mutu sebelum dipindahkan (migrasi) ke lingkungan produksi sesuai dengan pedoman pengembangan Sistem Elektronik dan *change management.*

7. Kebijakan dan Prosedur Pengelolaan Hubungan dengan Pihak Penyedia Jasa

   Apabila penyelenggaraan Teknologi Informasi BPR atau BPRS dilakukan oleh penyedia jasa Teknologi Informasi, BPR dan BPRS harus memantau dan mengevaluasi keandalan penyedia jasa dimaksud secara berkala baik yang menyangkut kinerja, reputasi penyedia jasa, dan kelangsungan penyediaan layanan. Untuk itu, BPR dan BPRS harus memiliki fungsi pengelolaan hubungan dengan pihak ketiga yang bertugas memantau layanan penyedia jasa Teknologi Informasi dengan menggunakan prosedur yang paling sedikit mencakup pemantauan layanan, pelaporan permasalahan, dan dokumentasi yang terkait dengan layanan penyedia jasa Teknologi Informasi.

BAB IV

JARINGAN KOMUNIKASI

Jaringan komunikasi merupakan hal yang sangat penting bagi industri keuangan. Hal tersebut dapat dilihat dari perkembangan produk dan aktivitas lembaga keuangan yang beragam dengan adanya jaringan komunikasi. Bahkan saat ini layanan perbankan sudah menjadi seperti tanpa batasan wilayah seiring berkembangnya jaringan komunikasi. BPR dan BPRS dapat menyediakan layanan perbankan elektronik secara *online* dan *realtime* seperti *Automated Teller Machine* (ATM), *internet Banking,* dan *mobile Banking*, baik milik BPR atau BPRS itu sendiri maupun milik penyedia jasa Teknologi Informasi.

Jaringan komunikasi termasuk hal yang perlu dipastikan integritasnya 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 karena jaringan komunikasi tersebut digunakan untuk mentransmisikan informasi berupa data, suara (*voice*), gambar (*image*) dan video yang rentan terhadap gangguan dan penyalahgunaan.

A. KEBIJAKAN DAN PROSEDUR JARINGAN KOMUNIKASI

BPR dan BPRS 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 BPR dan BPRS harus menetapkan *baseline*/standar yang digunakan secara intern untuk masing-masing *platform* (misalnya berdasarkan protokol atau sistem operasi) dan diterapkan di semua jaringan komunikasi yang digunakan oleh BPR atau BPRS.

Kebijakan dan prosedur yang perlu ditetapkan paling sedikit mencakup hal-hal sebagai berikut:

1. pengukuran kinerja dan perencanaan kapasitas jaringan (*performance and capacity planning*);

2. pengamanan jaringan komunikasi (*network access controls*, termasuk *remote access*);
3. *change management* (*setting, configuration, and testing*);
4. *network management, logging* dan *monitoring*;
5. penggunaan *internet*, *intranet*, surat elektronik, dan *wireless* (termasuk mekanisme penggunaan jaringan komunikasi);
6. tersedianya prosedur penyelesaian masalah (*trouble shooting*);
7. tersedianya fasilitas untuk rekam cadang dan pemulihan; dan
8. kecukupan kontrak dan tersedianya SLA yang sesuai dengan kebutuhan BPR dan BPRS dan harus dipantau secara berkala apabila jaringan komunikasi yang digunakan oleh BPR atau BPRS diselenggarakan oleh penyedia jasa Teknologi Informasi.

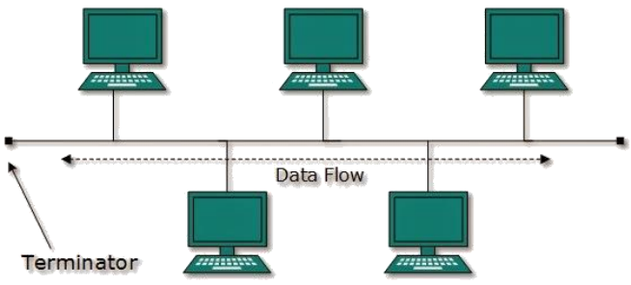
B. DESAIN JARINGAN KOMUNIKASI

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 diperhatikan, yaitu:

1. Penentuan Topologi Jaringan Komunikasi

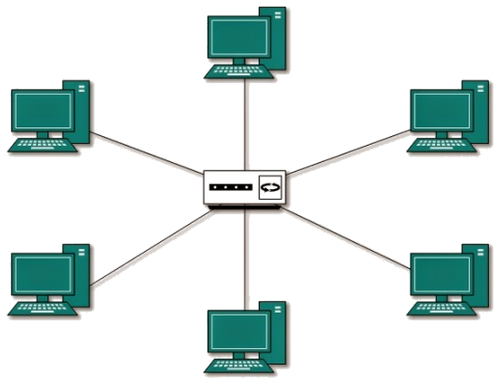
   Penggunaan topologi direncanakan sesuai dengan kebutuhan. Jenis-jenis topologi dimaksud antara lain:

   a. Topologi *Bus*



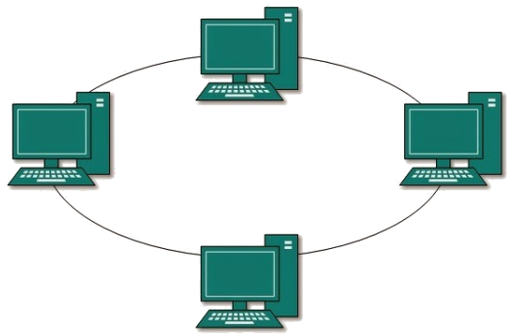
   Topologi *bus* adalah topologi yang hanya menggunakan sebuah kabel jenis *coaxial* disepanjang *node client*. Pada umumnya, ujung kabel *coaxial* tersebut biasanya dihubungkan dengan T-konektor sebagai kabel *end to end*.

b. Topologi *Star*



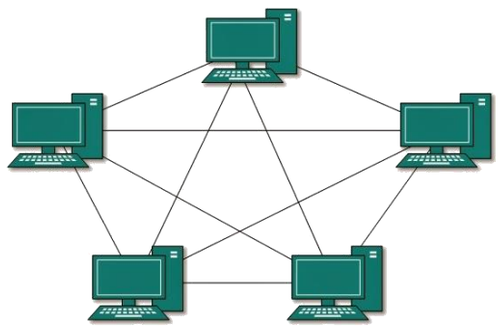
Topologi *star* atau bintang merupakan salah satu bentuk topologi jaringan yang menggunakan *switch*/*hub* untuk menghubungkan *client* satu dengan *client* lainnya.

c. Topologi *Ring*



Topologi *ring* atau cincin merupakan salah satu topologi jaringan yang menghubungkan satu komputer dengan komputer lainnya dalam suatu rangkaian melingkar menggunakan LAN *card* untuk menghubungkan komputer satu dengan komputer lainnya.

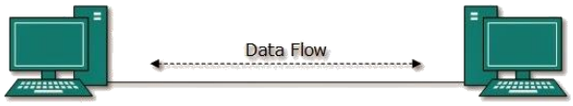
d. Topologi *Mesh*



Topologi *mesh* merupakan bentuk topologi yang cocok bagi jaringan komunikasi yang menghubungkan banyak komputer. Hal tersebut berfungsi sebagai jalur rekam

cadang pada saat jalur lain mengalami masalah.

e. Topologi *Peer to Peer*

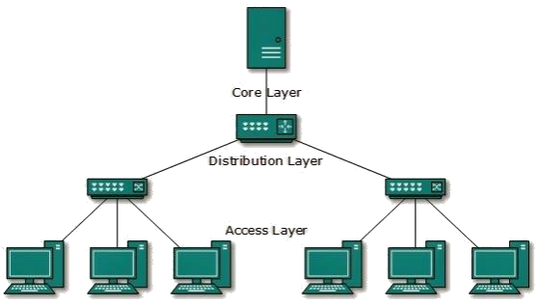


Topologi *peer to peer* merupakan topologi yang sederhana dikarenakan hanya menggunakan 2 buah komputer untuk saling terhubung, biasanya menggunakan satu kabel yang menghubungkan antar komputer untuk proses pertukaran data.

f. Topologi Linier

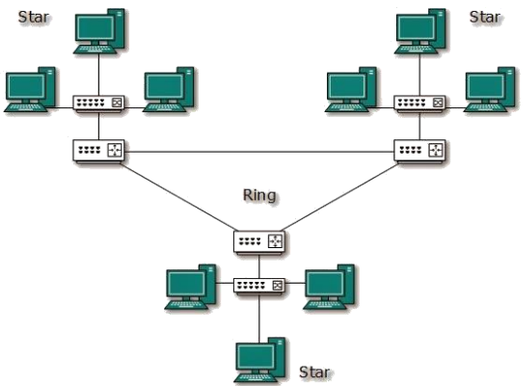
Topologi linier biasanya disebut dengan topologi *bus* beruntut. Pada topologi ini biasanya menggunakan satu kabel utama guna menghubungkan tiap titik sambungan pada setiap komputer.

g. Topologi *Tree*



Topologi *tree* atau pohon merupakan topologi gabungan antara topologi *star* dan topologi *bus*. Topologi ini biasanya digunakan untuk interkoneksi antar sentral dengan hirarki yang berbeda-beda.

h. Topologi *Hybrid*



Topologi *hybrid* merupakan topologi gabungan antara

beberapa topologi yang berbeda.

2. Perencanaan kapasitas (*capacity planning*) jaringan komunikasi. Perencanaan kapasitas jaringan komunikasi data dilakukan dengan memperhatikan riwayat penggunaan jaringan komunikasi data dan rencana bisnis BPR/BPRS.
3. Pemilihan media jaringan komunikasi.
4. Rekam cadang perangkat keras, *alternative routing* (jalur alternatif), atau *provider* alternatif.
5. Pengamanan fisik dan *logic* paling sedikit terdiri atas:
   a. penempatan perangkat jaringan pada lokasi yang aman terhadap gangguan alam dan akses oleh orang yang tidak berhak; dan
   b. pengaturan parameter sistem perangkat jaringan.
6. Tersedianya jejak audit, paling sedikit terhadap perubahan-perubahan pada *setting* parameter dan hak akses perangkat jaringan komunikasi dan juga penggunaan atas hak akses tersebut.

C. PENGENDALIAN AKSES JARINGAN KOMUNIKASI

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

1. akses ke jaringan komunikasi oleh pengguna didasarkan pada kebutuhan bisnis dengan memperhatikan aspek keamanan informasi;
2. melakukan pemisahan jaringan komunikasi berdasarkan segmen baik secara *logic* maupun fisik, misalnya pemisahan antara lingkungan pengembangan dan produksi;
3. dalam hal pemisahan secara fisik tidak dapat dilakukan, BPR dan BPRS harus memisahkan jaringan komunikasi secara *logic* dan memantau *security access* di jaringan komunikasi;

4. keputusan untuk terhubung ke jaringan komunikasi di luar BPR dan BPRS harus sesuai dengan persyaratan pengamanan dan secara formal disetujui oleh Direksi sebelum pelaksanaan;
5. menerapkan pengendalian yang dapat membatasi *network traffic* yang tidak sah atau tidak diharapkan;
6. konfigurasi perangkat jaringan komunikasi harus diatur dengan baik, termasuk fungsi-fungsi atau layanan 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; dan
9. pengujian secara berkala terhadap keamanan jaringan komunikasi, misalnya dengan *penetration testing*.

D. PENGENDALIAN, PENGAMANAN, DAN PEMELIHARAAN OPERASI JARINGAN KOMUNIKASI

Dalam melakukan pengendalian, pengamanan, dan pemeliharaan operasi jaringan komunikasi perlu diperhatikan antara lain:

1. tersedianya dokumentasi mengenai kebijakan dan prosedur operasional jaringan sesuai kebutuhan pengguna;
2. tersedianya rekam cadang perangkat keras/lunak, jaringan komunikasi Pangkalan Data serta pengaturan retensi dan pengelolaan data, termasuk mekanisme *restart/recovery* yang telah teruji;
3. akses terhadap jaringan dibatasi hanya kepada pengguna yang berwenang melalui penelaahan "*user profile*" secara berkala, termasuk pengamanan terhadap setiap penggunaan perintah sistem (*system command*) yang dalam hal ini perlu dibuat laporan oleh satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi atas setiap penyalahgunaan akses;
4. pelatihan yang memadai bagi satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi

Informasi perlu diselenggarakan agar mampu memberikan dukungan terhadap kelancaran operasional jaringan;

5. evaluasi terhadap pelaksanaan implementasi operasional jaringan untuk menilai kesesuaian dengan kebutuhan satuan kerja pengguna dan tindak lanjut apabila diperlukan penyempurnaan;
6. perlu adanya mekanisme pemantauan secara cepat dan akurat untuk menjamin efektivitas dan efisiensi pengoperasian jaringan antara lain mencakup prioritas proses, *response time,* dan kapasitas perangkat keras/lunak;
7. tersedianya prosedur Rencana Pemulihan Bencana yang terutama mencakup rekam cadang terhadap perangkat keras/lunak, Pangkalan Data, serta mekanisme *restart/recovery,* yang membutuhkan pengujian secara berkala; dan
8. tersedianya alternatif sistem komunikasi untuk mengantisipasi jika sistem yang ada mengalami gangguan.

E. PEMANTAUAN JARINGAN KOMUNIKASI

Dalam pemantauan jaringan komunikasi yang digunakan oleh BPR dan BPRS perlu diperhatikan antara lain:

1. jejak audit yang tersedia harus dipantau secara teratur untuk dapat mendeteksi secara dini ada tidaknya penyimpangan;
2. kinerja jaringan komunikasi diukur secara berkala berdasarkan tingkat ketersediaan (*availability*) dan *response time*;
3. BPR dan BPRS harus memantau kapasitas yang digunakan dan yang diperlukan untuk rencana pengembangan bisnis dibandingkan dengan kapasitas terpasang;
4. BPR dan BPRS harus memantau dan menindaklanjuti penyusupan/serangan terhadap jaringan komunikasi; dan
5. BPR dan BPRS harus melakukan kaji ulang pemberian akses ke pengguna secara berkala untuk meyakinkan bahwa akses yang diberikan masih sesuai dengan tugas dan wewenangnya, serta perlu dilakukan kaji ulang atas pengguna jaringan komunikasi di BPR atau BPRS yang memiliki akses ke jaringan komunikasi di luar BPR atau BPRS.

F. PERANGKAT LUNAK JARINGAN KOMUNIKASI

Dalam memantau dan melakukan pengendalian dan pengamanan terhadap perangkat lunak jaringan komunikasi, BPR dan BPRS perlu memperhatikan paling sedikit:

1. transmisi data termasuk proses dalam keadaan darurat, otorisasi dan jejak audit, proteksi transmisi data yang sensitif, serta akses terhadap *utilities* yang tersedia; dan
2. pemeliharaan perangkat lunak jaringan komunikasi.

G. PENGAMANAN DATA JARINGAN KOMUNIKASI

Dalam pengamanan data jaringan komunikasi, perlu diperhatikan mengenai pengamanan data yang ditransmisikan dengan menggunakan teknik enkripsi data serta pengamanan jaringan baik fisik maupun *logic*.

H. DOKUMENTASI JARINGAN KOMUNIKASI

Dalam kegiatan pengelolaan jaringan komunikasi, BPR dan BPRS harus melakukan dokumentasi antara lain terhadap hal-hal sebagai berikut:

1. kebijakan, prosedur, dan *baseline*/standar tentang jaringan komunikasi;
2. diagram jaringan komunikasi secara rinci;
3. daftar dan spesifikasi perangkat lunak dan perangkat keras jaringan komunikasi;
4. daftar permasalahan dan penanganannya;
5. laporan pemantauan jaringan komunikasi;
6. laporan perencanaan kapasitas jaringan komunikasi;
7. kontrak dan SLA dengan pihak ketiga penyedia jasa fasilitas jaringan komunikasi;
8. dokumen pengujian jaringan komunikasi;
9. dokumen implementasi jaringan komunikasi;
10. dokumen perubahan jaringan komunikasi disertai alasannya; dan
11. daftar pengguna dan wewenangnya.

BAB V

PENGAMANAN INFORMASI

Informasi merupakan hal penting bagi BPR dan BPRS, 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 BPR atau BPRS, nasabah, bank lain, dan terhadap sistem perbankan nasional. Informasi harus dilindungi atau diamankan oleh seluruh personil di BPR atau BPRS.

Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen Teknologi Informasi terkait, seperti perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC, dan lain-lain) dan sumber daya manusia (termasuk kualifikasi dan keterampilan).

A. PRINSIP PENGAMANAN INFORMASI

Pengamanan informasi paling sedikit memperhatikan prinsip-prinsip sebagai berikut:

1. dilaksanakan untuk meyakini bahwa informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan dapat ditelusurinya suatu informasi elektronik dan/atau dokumen elektronik yang terkait dengan nasabah dan seluruh aktivitas BPR atau BPRS secara efektif dan efisien sesuai dengan ketentuan peraturan perundang-undangan;
2. memperhatikan aspek sumber daya manusia, proses, dan teknologi;
3. menerapkan pengamanan informasi secara komprehensif dan berkesinambungan yaitu dengan menetapkan tujuan dan kebijakan pengamanan informasi, implementasi pengendalian pengamanan informasi, memantau dan mengevaluasi kinerja dan efektivitas kebijakan pengamanan informasi, serta melakukan penyempurnaan.

Selain hal-hal tersebut di atas, BPR dan BPRS perlu mempertimbangkan implementasi standar internasional di bidang pengamanan informasi antara lain *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC), *Control Objective For Information and Related Technology* (COBIT), *Information Technology Infrastructure Library* (IT-IL), dan standar nasional seperti Standar Nasional Indonesia (SNI), dengan memperhatikan kompleksitas usaha yang meliputi antara lain keragaman dalam jenis transaksi/produk/jasa dan jaringan kantor serta teknologi pendukung yang digunakan.

B. KEBIJAKAN PENGAMANAN INFORMASI

Direksi BPR dan BPRS harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus dikomunikasikan secara berkala kepada seluruh pegawai BPR atau BPRS dan pihak ekstern yang terkait. Disamping itu dilakukan evaluasi secara berkala dan evaluasi apabila terdapat perubahan penting. Kebijakan tentang pengamanan informasi paling sedikit mencakup:

1. tujuan pengamanan informasi yang paling sedikit meliputi pengelolaan aset, sumber daya manusia, pengamanan fisik, pengamanan *logic* (*logical security*), pengamanan operasional Teknologi Informasi, penanganan insiden, pengamanan informasi, dan pengamanan informasi dalam pengembangan sistem;
2. komitmen Direksi terhadap pengamanan informasi sejalan dengan strategi dan tujuan bisnis;
3. 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;
4. tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi; dan
5. dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

C. PROSEDUR PENGAMANAN INFORMASI

1. Pengelolaan Aset

   a) aset BPR dan BPRS yang terkait dengan informasi harus diidentifikasikan, ditentukan pemilik/penanggung jawabnya 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 antara lain:

      1) informasi rahasia, misalnya data simpanan nasabah, data pribadi nasabah;
      2) informasi intern, misalnya peraturan tentang gaji pegawai BPR atau BPRS; dan
      3) informasi biasa, misalnya informasi tentang produk BPR atau BPRS yang ditawarkan ke masyarakat.

      Klasifikasi dapat dibuat berdasarkan nilai, sensitivitas, hukum/ketentuan, dan tingkat kepentingan bagi BPR atau BPRS.

2. Pengelolaan Sumber Daya Manusia

   a) sumber daya manusia baik pegawai BPR atau BPRS, konsultan, pegawai honorer dan pegawai penyedia jasa Teknologi Informasi yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi;

   b) peran dan tanggung jawab sumber daya manusia baik pegawai BPR atau BPRS, konsultan, pegawai honorer, dan pegawai penyedia jasa Teknologi Informasi yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi;

   c) dalam perjanjian kerja sama atau kontrak dengan pegawai BPR atau BPRS, konsultan, pegawai honorer, dan pegawai

penyedia jasa Teknologi Informasi harus tercantum ketentuan-ketentuan mengenai pengamanan informasi yang sesuai dengan kebijakan pengamanan informasi BPR atau BPRS. Sebagai contoh, perlu adanya klausula yang menyatakan bahwa pegawai BPR atau BPRS, konsultan, pegawai honorer, dan pegawai penyedia jasa Teknologi Informasi harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi;

d) selain perjanjian kerja sama antara BPR atau BPRS dengan penyedia jasa Teknologi Informasi, semua pegawai penyedia jasa Teknologi Informasi yang ditugaskan di BPR atau BPRS harus menandatangani suatu perjanjian menjaga kerahasiaan informasi (*non-disclosure agreement*);

e) pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai BPR atau BPRS, konsultan, pegawai honorer, dan pegawai penyedia jasa Teknologi Informasi. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab masing-masing pihak;

f) BPR dan BPRS harus menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi;

g) BPR dan BPRS harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan perubahan/penutupan hak akses pegawai BPR atau BPRS, konsultan, pegawai honorer dan pegawai penyedia jasa Teknologi Informasi yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak.

h) BPR dan BPRS harus menetapkan pemisahan tugas dan tanggung jawab (*segregation of duties*), yaitu memastikan terdapat pemisahan tugas dan tanggung jawab antara sumber daya manusia di operasional BPR atau BPRS.

3. Pengamanan Fisik dan Lingkungan

a) fasilitas pemrosesan informasi yang penting (misalnya *mainframe,* peladen, komputer, 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*, *Personal Identification Number/*PIN, *biometrics*), kelengkapan alat pengamanan di dalam ruangan (misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, CCTV) serta pemeliharaan kebersihan ruangan dan peralatan (misalnya dari debu, rokok, makanan/minuman, barang mudah terbakar);

c) fasilitas pendukung seperti AC, sumber daya listrik, dan pendeteksi dan pemadam api harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;

d) aset milik penyedia jasa Teknologi Informasi (misalnya peladen, *switching tools*) harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai seperti misalnya dengan menerapkan pengamanan yang cukup, *dual control*, atau menempatkan secara terpisah dari aset milik BPR atau BPRS;

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

4. Pengamanan Logic (*Logic Security*)

a) BPR dan BPRS harus memiliki prosedur formal secara tertulis yang telah disetujui oleh Direksi tentang pengadministrasian pengguna yang meliputi pendaftaran, perubahan dan penghapusan pengguna, baik untuk pengguna intern maupun ekstern BPR atau BPRS**,** (misalnya penyedia jasa Teknologi Informasi).

b) BPR dan BPRS harus menetapkan prosedur pengendalian melalui pemberian *password* awal (*initial password*) kepada

pengguna dengan memperhatikan paling sedikit 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 pengguna dan tidak mudah ditebak;
4) pemilik *user-id* terutama dari pegawai BPR atau BPRS, pegawai honorer, dan pegawai penyedia jasa Teknologi Informasi 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 BPR atau BPRS sebelum diimplementasikan dan sedapat mungkin mengganti *user-id* standar dari sistem (*default user-id*).

c) BPR dan BPRS harus mewajibkan pengguna 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 paling sedikit kombinasi 2 tipe karakter (huruf, angka, atau karakter khusus);
      (c) tidak didasarkan atas data pribadi pengguna 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; dan
   5) menghindari penggunaan *password* yang sama secara berulang.

d) BPR dan BPRS harus menonaktifkan hak akses jika *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) BPR dan BPRS harus melakukan pemeriksaan/*review* berkala terhadap hak akses pengguna untuk memastikan bahwa hak akses yang diberikan sesuai dengan wewenang yang diberikan.

f) sistem operasi, sistem aplikasi, Pangkalan Data, *utility,* dan perangkat lainnya yang dimiliki oleh BPR dan BPRS sedapat mungkin membantu pelaksanaan pengamanan *password*, sebagai contoh:

   1) memaksa pengguna untuk mengubah *password* setelah jangka waktu tertentu dan menolak bila pengguna memasukkan *password* yang sama dengan yang digunakan sebelumnya saat mengganti *password*;
   2) menyimpan *password* secara aman (ter-enkripsi);
   3) memutuskan hubungan atau akses pengguna jika tidak terdapat respon selama jangka waktu tertentu (*session time-out*);
   4) menonaktifkan atau menghapus hak akses pengguna jika pengguna tidak melakukan *login* melebihi jangka waktu tertentu (*expiration interval*), misalnya karena cuti atau pindah bagian.

g) BPR dan BPRS harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai dalam penggunaan perangkat *mobile computing* dan media penyimpan data seperti *notebook, hand phone, flash disk, external hard disk,* dan media lainnya, termasuk bila menggunakan *wireless access* atau *wireless network*.

h) BPR dan BPRS 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) BPR dan BPRS yang menggunakan *file sharing* harus menetapkan pembatasan akses paling sedikit melalui penggunaan *password* dan pengaturan pihak yang berwenang melakukan akses.

j) BPR dan BPRS perlu memperhatikan proses *security hardening* terhadap perangkat keras dan perangkat lunak, seperti *setting parameter* atau *patch*.

5. Pengamanan Operasional Teknologi Informasi

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

a) informasi dan perangkat lunak harus dibuatkan rekam cadang dan prosedur pemulihan yang teruji sesuai dengan tingkat kepentingannya;

b) BPR dan BPRS perlu mengantisipasi dan menerapkan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, Pangkalan Data 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) BPR dan BPRS harus memiliki kebijakan dan prosedur pengkinian *anti-virus* dan *patch* serta memastikan pelaksanaannya;

d) BPR dan BPRS harus membuat prosedur yang mencakup identifikasi *patch* yang ada, melakukan pengujian, dan menginstalasinya jika memang dibutuhkan;

e) BPR dan BPRS 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) BPR dan BPRS harus menetapkan penggunaan enkripsi dengan menggunakan teknik kriptografi tertentu dalam mengamankan proses transmisi informasi yang sensitif, khususnya yang melalui jaringan di luar jaringan komunikasi BPR atau BPRS, 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) BPR dan BPRS 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 "kritikal".

Contoh metode identifikasi dan otentikasi antara lain *login id* dan *password, token device* atau *biometrics* (misalnya *fingerprint, retina scan, face/iris/hand/palm analysis, signature recognition, voice recognition*); dan

h) BPR dan BPRS 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.

6. Penanganan Insiden dalam Pengamanan Informasi

Hal-hal yang harus diperhatikan BPR dan BPRS 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) BPR dan BPRS 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) analisis atas insiden untuk mencegah terulangnya insiden; dan
5) pendokumentasian bukti terkait insiden dan tindak lanjutnya.

c) BPR dan BPRS perlu mempertimbangkan pembentukan tim khusus yang menangani insiden pengamanan oleh TRIPI (Tim Respon Insiden dalam Pengamanan Informasi) sesuai dengan skala usaha dan kompleksitas penyelenggaraan Teknologi Informasi BPR atau BPRS;

d) pegawai BPR atau BPRS, pegawai honorer, dan pegawai penyedia jasa Teknologi Informasi diminta untuk melaporkan setiap kali menemukan indikasi atau potensi kelemahan pada Sistem Elektronik sesuai kebijakan dan prosedur pelaporan insiden pengamanan. Kelemahan yang perlu dilaporkan misalnya adanya *virus* dari surat elektronik yang masuk.

7. Rekam Cadang dan Uji *Restore*

Rekam cadang dan uji *restore* diperlukan untuk menjamin tersedianya data untuk kelangsungan operasional BPR atau BPRS, baik dalam operasional secara rutin maupun apabila terjadi gangguan kerusakan terhadap data sehingga kerugian yang lebih besar dapat dihindarkan. Dalam hal ini rekam cadang dan uji *restore* dimaksud meliputi data, *file*, aplikasi, sistem operasi, dan dokumen lainnya, harus disimpan di lokasi/gedung yang terpisah. Hal-hal tersebut di atas adalah beberapa contoh kontrol dan teknologi yang dapat digunakan untuk membantu pengamanan informasi.

8. Retensi Data

Retensi data dilakukan untuk mempertahankan integritas data yang di rekam cadang dalam jangka waktu tertentu. Jangka waktu retensi data disesuaikan dengan ketentuan peraturan perundang-undangan yang mengatur mengenai dokumen perusahaan.

9. Lainnya

Pengamanan informasi juga perlu diterapkan dalam aspek lain seperti pengembangan dan pengadaan Sistem Elektronik termasuk Aplikasi Inti Perbankan, jaringan komunikasi data, rencana pemulihan bencana, dan kegiatan kerja sama dengan penyedia jasa Teknologi Informasi atau penyedia Aplikasi Inti Perbankan.

BAB VI

RENCANA PEMULIHAN BENCANA

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 BPR atau BPRS, tetapi juga berdampak pada kegiatan operasional bisnis BPR atau BPRS terutama pelayanan kepada nasabah. Bila tidak ditangani secara khusus, selain BPR atau BPRS akan menghadapi risiko operasional, BPR dan BPRS juga dapat menghadapi risiko reputasi yang berdampak pada menurunnya tingkat kepercayaan nasabah kepada BPR atau BPRS.

Untuk meminimalisasi risiko tersebut, BPR dan BPRS diharapkan memiliki *Business Continuity Management* (BCM) yaitu proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional BPR atau BPRS tetap dapat berfungsi walaupun menghadapi gangguan/bencana guna melindungi kepentingan para pemangku kepentingan. BCM yang efektif perlu didukung dengan beberapa hal salah satunya adalah penyusunan *Business Continuity Plan* (BCP).

Komponen prosedur BCP yang wajib dimiliki oleh BPR dan BPRS adalah Rencana Pemulihan Bencana (*Disaster Recovery Plan*) sesuai dengan POJK SPTI. Rencana Pemulihan Bencana adalah dokumen yang berisikan rencana dan langkah-langkah memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar BPR dan BPRS dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana. Rencana Pemulihan Bencana lebih menekankan pada aspek teknologi dengan fokus pada *data recovery/restoration plan* dan berfungsinya sistem aplikasi dan infrastruktur Teknologi Informasi yang kritikal.

A. KEBIJAKAN DAN PROSEDUR RENCANA PEMULIHAN BENCANA

Direksi BPR dan BPRS harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap rencana pemulihan bencana yang mencakup:

1. Analisis terhadap Rencana Pemulihan Bencana

   Analisis terhadap kemungkinan timbulnya risiko yang dapat disebabkan oleh faktor antara lain:

   a) faktor kebakaran;
   b) faktor alam, seperti banjir dan gempa;
   c) faktor teknis, seperti kerusakan perangkat keras/lunak, gangguan tenaga listrik, atau gangguan transmisi data; dan/atau
   d) faktor manusia, seperti sabotase.

2. Jenis Prosedur Rencana Pemulihan Bencana

   Adapun jenis-jenis prosedur dalam Rencana Pemulihan Bencana antara lain mencakup:

   a) prosedur tanggap darurat (*emergency response - immediate steps*) untuk mengendalikan sistem pada saat terjadi gangguan/bencana, mengurangi dampak kerugian, serta menentukan status keadaan bencana;
   b) prosedur pemulihan sistem yang memungkinkan kegiatan operasional BPR atau BPRS dapat kembali ke kondisi normal; dan/atau
   c) prosedur sinkronisasi data digunakan untuk memastikan kesamaan antara data mesin yang digunakan untuk operasional dengan data rekam cadang, serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem.

3. Komponen Prosedur Rencana Pemulihan Bencana

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

   a) Personel

      Rencana Pemulihan Bencana harus secara jelas mengemukakan komposisi, wewenang, dan tanggung jawab setiap personel yang berkaitan dengan penyelenggaraan

Teknologi Informasi dan memiliki alur komunikasi yang memadai.

b) Teknologi dan Aplikasi Utama

Prosedur yang disusun harus memperhatikan komponen teknologi yang dimiliki BPR atau BPRS seperti perangkat keras, perangkat lunak, dan fasilitas komunikasi BPR atau BPRS.

Selanjutnya BPR dan BPRS harus memiliki prosedur dan dokumentasi yang lengkap untuk memulihkan aplikasi-aplikasi utama yang terkait dengan Aplikasi Inti Perbankan maupun operasional BPR atau BPRS lainnya.

Selain itu hal-hal yang berkaitan dengan data juga perlu diperhatikan seperti dokumentasi sistem dan data rekam cadang.

c) Pusat Pemulihan Bencana (*Disaster Recovery Center*/DRC)

Bagi BPR dan BPRS yang memiliki Pusat Pemulihan Bencana, BPR dan BPRS harus memastikan ketersediaan Pusat Pemulihan Bencana sebagai rekam cadang Pusat Data yang dapat dioperasikan apabila Pusat Data tidak dapat beroperasi (dalam kondisi bencana*)*. Sesuai dengan alternatif strategi yang dipilih BPR dan BPRS, Pusat Pemulihan Bencana dapat dikelola sendiri maupun oleh penyedia jasa Teknologi Informasi dengan memperhatikan hal-hal sebagai berikut:

(1) Pusat Pemulihan Bencana hendaknya ditempatkan pada lokasi yang terpisah dari lokasi Pusat Data, dengan memperhatikan karakteristik risiko berdasarkan:

(a) analisis risiko yang berkaitan dengan lokasi Pusat Pemulihan Bencana (apakah wilayah gempa, petir, banjir, huru hara, kerusuhan, dan gangguan lain) dan terhubung dengan infrastruktur komunikasi dan listrik yang berbeda dengan Pusat Data, serta fasilitas lain yang diperlukan untuk tetap berjalannya suatu sistem; dan

(b) jangkauan geografi atas suatu gangguan/bencana dan dampaknya terhadap kota atau wilayah tempat lokasi Pusat Pemulihan Bencana berada.

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

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

(4) merupakan *restricted area*; dan

(5) memperhitungkan waktu tempuh untuk terjaminnya proses *recovery*.

d) Rekam Cadang Dokumentasi, Sistem, dan Data

BPR dan BPRS harus memastikan ketersediaan rekam cadang yang efektif dari informasi bisnis yang penting, perangkat lunak dan dokumentasi terkait sistem, dan pengguna untuk setiap proses fungsi bisnis yang penting (*critical*). Hal-hal yang harus diperhatikan dalam dokumentasi, sistem, dan data rekam cadang antara lain mencakup:

1) rekam cadang tersebut harus disimpan di lokasi terpisah dari Pusat Data (*off site*) yang memenuhi standar sistem pengamanan yang memadai, serta setiap perubahan dan modifikasi harus didokumentasikan dan salinannya juga harus diperbaharui;

2) rekam cadang sistem secara menyeluruh (*full system backup*) harus dilakukan secara periodik atau jika terjadi perubahan sistem yang mendasar, rekam cadang tersebut harus dilakukan sesegera mungkin;

3) seluruh media rekam cadang menggunakan standar penamaan untuk dapat mengidentifikasi penggunaan, tanggal, dan jadwal retensi;

4) media rekam cadang harus dilakukan uji *restore* secara periodik untuk memastikan rekam cadang dapat

digunakan pada saat diperlukan (keadaan *emergency*); dan

5) BPR dan BPRS harus memiliki prosedur untuk *disposal* media rekam cadang.

e) Fasilitas Komunikasi

BPR dan BPRS harus memastikan tersedianya alternatif jalur komunikasi di wilayah operasional BPR atau BPRS yang dapat digunakan di lingkungan intern maupun dengan pihak ekstern pada saat gangguan/bencana.

4. Penetapan Kejelasan Tanggung Jawab bagi Pihak-Pihak Terkait dalam Penyelenggaraan Rencana Pemulihan Bencana.

a) Tanggung jawab Direksi BPR dan BPRS paling sedikit meliputi:

1) menetapkan kebijakan dan prosedur tertulis mengenai Rencana Pemulihan Bencana;
2) menelaah dan menyetujui Rencana Pemulihan Bencana;
3) melakukan evaluasi terhadap kelayakan Rencana Pemulihan Bencana milik penyedia jasa Teknologi Informasi dalam hal BPR atau BPRS melakukan kerja sama dengan penyedia jasa Teknologi Informasi; dan
4) menetapkan tingkat gangguan dan bencana serta pemulihannya.

b) Tanggung jawab satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi paling sedikit meliputi:

1) tanggung jawab penuh terhadap efektivitas penyelenggaraan Rencana Pemulihan Bencana, termasuk memastikan setiap pihak dalam BPR atau BPRS memiliki kesadaran atas penerapan Rencana Pemulihan Bencana;
2) penentuan skenario pemulihan yang akan digunakan apabila terjadi gangguan atau bencana berdasarkan prioritisasi atas Sistem Elektronik yang dianggap kritis; dan

3) evaluasi laporan mengenai setiap tahapan dalam pengujian dan pelaksanaan Rencana Pemulihan Bencana.

B. DOKUMENTASI STRATEGI DAN PROSEDUR UNTUK PEMULIHAN (*RECOVERY*)

BPR dan BPRS harus mendokumentasikan strategi dan prosedur untuk proses pemulihan yang mencakup:

1. prosedur untuk melaksanakan Rencana Pemulihan Bencana;
2. prioritas pengolahan;
3. sumber daya yang diperlukan (termasuk perangkat keras/lunak dan lokasi peladen); dan
4. data.

C. UJI COBA RENCANA PEMULIHAN BENCANA

Uji coba Rencana Pemulihan Bencana diperlukan untuk memastikan bahwa Rencana Pemulihan Bencana dapat dioperasikan dengan baik pada saat terjadi gangguan/bencana. BPR dan BPRS melakukan uji coba terhadap Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 3 (tiga) tahun. Uji coba dilakukan terhadap seluruh sistem/aplikasi kritikal dan infrastruktur yang kritikal serta melibatkan pengguna Teknologi Informasi.

Yang dimaksud dengan sistem/aplikasi dan infrastruktur yang kritikal adalah sistem/aplikasi dan infrastruktur yang dapat mengganggu layanan operasional bank sehingga berpotensi menimbulkan risiko reputasi.

BPR dan BPRS melakukan kaji ulang terhadap Rencana Pemulihan Bencana dilakukan secara berkala paling sedikit 1 (satu) kali dalam 3 (tiga) tahun dengan mempertimbangkan hasil uji coba, termasuk dalam hal BPR dan BPRS melakukan perubahan yang signifikan terhadap sistem, aplikasi, atau infrastruktur Teknologi Informasi, misalnya perubahan pada Aplikasi Inti Perbankan.

Apabila BPR dan BPRS menggunakan penyedia jasa Teknologi Informasi dalam kegiatan operasional, uji coba yang dilakukan juga perlu melibatkan penyedia jasa dimaksud.

1. Ruang Lingkup Uji Coba

   BPR dan BPRS harus secara jelas menentukan fungsi, sistem, dan proses yang akan dilakukan uji coba. Hal-hal yang perlu diuji coba antara lain meliputi efektivitas dari:

   a) prosedur penetapan tingkat gangguan dan bencana;
   b) fasilitas Pusat Pemulihan Bencana yang disediakan oleh penyedia jasa Teknologi Informasi baik yang digunakan untuk BPR dan BPRS sendiri maupun yang digunakan bersama dengan BPR dan BPRS lain;
   c) prosedur pemulihan operasional Teknologi Informasi; dan
   d) pemulihan Pusat Data.

   Uji coba yang dilakukan harus didokumentasikan secara tertib dan dievaluasi untuk memastikan efektivitas dan keberhasilan uji coba. Dalam hal dalam uji coba terdapat kelemahan atas Rencana Pemulihan Bencana, Rencana Pemulihan Bencana perlu disempurnakan.

2. Skenario Uji Coba

   BPR dan BPRS harus memiliki skenario uji coba yang menyeluruh dan mencakup seluruh kondisi yang mungkin terjadi untuk setiap uji coba yang akan dilakukan. Pelaksanaan skenario tersebut tidak boleh mengganggu kegiatan operasional BPR atau BPRS. Pelaksanaan skenario uji coba diharapkan dapat mendeteksi adanya kelemahan dari prosedur yang ada dalam rangka perbaikan Rencana Pemulihan Bencana.

3. Analisis dan Laporan Hasil Uji Coba

   Hasil uji coba dan analisis dari setiap permasalahan yang ditemukan pada saat uji coba harus dilaporkan kepada Direksi. Hal-hal yang dilaporkan paling sedikit mencakup:

   a) penilaian ketercapaian tujuan uji coba;
   b) penilaian atas validitas uji coba pemrosesan data;
   c) tindakan korektif untuk mengatasi permasalahan yang terjadi;
   d) deskripsi mengenai perbandingan antara hasil dari Rencana Pemulihan Bencana dengan sistem yang digunakan dan

hasil uji coba serta usulan perubahannya apabila terdapat perbedaan; dan

e) rekomendasi untuk uji coba selanjutnya.

Dalam hal berdasarkan hasil uji coba ditemukan kegagalan, BPR dan BPRS harus mengkaji penyebab kegagalan atau permasalahan yang terjadi dan melakukan uji coba ulang.

D. PEMELIHARAAN RENCANA PEMULIHAN BENCANA

BPR dan BPRS harus memastikan bahwa Rencana Pemulihan Bencana dapat dijalankan setiap saat antara lain dengan meningkatkan pemahaman kepada seluruh jenjang organisasi di BPR atau BPRS maupun di penyedia jasa Teknologi Informasi atas pentingnya Rencana Pemulihan Bencana dan berpartisipasi aktif dalam pelaksanaan Rencana Pemulihan Bencana khususnya satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.

BPR dan BPRS harus melakukan pengkinian Rencana Pemulihan Bencana untuk memastikan kesesuaiannya dengan kondisi saat ini. Dalam melakukan pengkinian, hal-hal yang perlu diperhatikan antara lain perubahan yang ada dalam sistem, perangkat lunak, sistem operasi, perangkat keras, pihak-pihak lain terkait (*counter parties*), dan penyedia layanan (*services provider*). Perubahan tersebut harus dianalisis pengaruhnya terhadap Rencana Pemulihan Bencana yang ada saat ini dan menentukan perbaikan yang dibutuhkan untuk mengakomodasi perubahan tersebut. Selanjutnya Rencana Pemulihan Bencana hasil pengkinian tersebut harus didokumentasikan dan didistribusikan ke seluruh jenjang organisasi BPR atau BPRS.

BAB VII

AUDIT INTERN TEKNOLOGI INFORMASI

Sistem pengendalian intern yang efektif merupakan komponen penting dalam pengelolaan BPR dan BPRS serta menjadi dasar bagi kegiatan operasional BPR dan BPRS yang sehat dan aman. Sistem pengendalian intern yang efektif dapat membantu BPR atau BPRS dalam menjaga aset, menjamin tersedianya pelaporan keuangan dan manajerial yang dapat dipercaya, meningkatkan kepatuhan BPR dan BPRS terhadap ketentuan dan peraturan perundang-undangan, serta mengurangi risiko terjadinya kerugian, penyimpangan, dan pelanggaran aspek kehati-hatian.

Penggunaan sarana Teknologi Informasi disamping meningkatkan kemampuan BPR dan BPRS dalam melaksanakan kegiatan operasional, juga mengandung risiko yang dapat mengakibatkan kerugian, baik yang bersifat finansial maupun non-finansial. Oleh karena itu, sistem pengendalian intern perlu diterapkan sebagai salah satu upaya meminimalkan kerugian dimaksud.

Fungsi audit intern merupakan salah satu bagian dari sistem pengendalian intern. Pelaksanaan fungsi audit intern dilakukan dalam rangka melakukan evaluasi terhadap penyelenggaraan Teknologi Informasi secara independen dan objektif untuk meningkatkan efisiensi dan efektivitas, pengendalian intern, dan tata kelola yang baik.

A. ORGAN PELAKSANA FUNGSI AUDIT INTERN TERHADAP PENYELENGGARAAN TEKNOLOGI INFORMASI

Fungsi audit intern terhadap penyelenggaraan Teknologi Informasi harus dilakukan dengan pelaksanaan sebagai berikut:

1. bagi BPR, fungsi audit intern terhadap penyelenggaraan Teknologi Informasi dilakukan:
   a) sebagai bagian dari audit intern BPR sesuai dengan Peraturan Otoritas Jasa Keuangan yang mengatur mengenai penerapan tata kelola bagi BPR; atau
   b) secara terpisah dari pelaksanaan audit intern BPR dalam hal audit penyelenggaraan Teknologi Informasi dilakukan oleh auditor ekstern;

2. bagi BPRS, fungsi audit intern terhadap penyelenggaraan Teknologi Informasi tetap dilakukan dengan mengacu pada ketentuan mengenai penerapan tata kelola BPRS dan peraturan perundang-undangan terkait lainnya. Pelaksanaan fungsi audit intern terhadap penyelenggaraan Teknologi Informasi tersebut dapat dilaksanakan sendiri oleh BPRS yang bersangkutan atau menggunakan jasa auditor ekstern;

Pelaksanaan fungsi audit intern dilakukan oleh Satuan Kerja Audit Intern atau Pejabat Eksekutif yang bertanggung jawab terhadap pelaksanaan fungsi audit intern, yang disebut dengan organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi.

B. PEDOMAN AUDIT INTERN TERHADAP PENYELENGGARAAN TEKNOLOGI INFORMASI

1. Kebijakan Umum Audit

Pedoman audit intern terhadap penyelenggaraan Teknologi Informasi paling sedikit mencakup kebijakan umum mengenai:

a) pernyataan visi dan misi fungsi audit intern penyelenggaraan Teknologi Informasi;
b) struktur organisasi dan sistem pelaporan;
c) penentuan frekuensi dan jadwal audit yang paling sedikit akan diterapkan BPR atau BPRS untuk audit intern penyelenggaraan Teknologi Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun sebagai bagian dari pelaksanaan audit intern atau dilaksanakan terpisah dari audit intern; dan
d) pelaksanaan audit intern dilakukan terhadap aspek terkait Teknologi Informasi sesuai kebutuhan, prioritas, dan hasil analisis risiko Teknologi Informasi BPR atau BPRS paling sedikit mencakup aspek sebagai berikut:
    1) Aplikasi Inti Perbankan, untuk memastikan kesesuaian Aplikasi Inti Perbankan telah memenuhi standar minimal sebagai berikut:
        (a) menerapkan ketentuan peraturan perundang-undangan bagi BPR atau BPRS;

(b) melakukan pembukuan transaksi antar jaringan kantor:

(1) pada hari yang sama bagi BPR dan BPRS yang tidak menyediakan layanan perbankan elektronik (*electronic banking*) dan tidak melakukan kegiatan sebagai penerbit kartu *Automated Teller Machine* (ATM);

(2) secara *online* dan *real time* bagi BPR dan BPRS yang menyediakan layanan perbankan elektronik dan/atau melakukan kegiatan sebagai penerbit kartu *Automated Teller Machine* (ATM).

Layanan perbankan elektronik sebagaimana dimaksud pada angka (1) dan (2) termasuk juga kegiatan sebagai penerbit kartu debet sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan yang mengatur mengenai kegiatan usaha dan wilayah jaringan kantor BPR berdasarkan modal inti bagi BPR dan Peraturan Otoritas Jasa Keuangan yang mengatur mengenai Bank Pembiayaan Rakyat Syariah bagi BPRS.

(c) menghasilkan data dan informasi yang digunakan dalam mendukung proses penyusunan laporan untuk kebutuhan intern dan ekstern;

(d) mengonsolidasikan fungsi-fungsi yang terdapat dalam Aplikasi Inti Perbankan untuk mendukung penyediaan data dan informasi yang lengkap, akurat, kini, dan utuh; dan

(e) mampu mengimplementasikan profil nasabah secara terpadu (*Single Customer Identification File*).

2) wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi, untuk memastikan pelaksanaan wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan

Teknologi Informasi sebagaimana dimaksud dalam Bab I.

e) Selain aspek tersebut dalam huruf d. angka 1) dan 2), BPR dan BPRS dapat melakukan audit terhadap aspek penyelenggaraan Teknologi Informasi sebagai berikut:
   (a) pengembangan dan pengadaan Teknologi Informasi, untuk memastikan pengembangan dan pengadaan Teknologi Informasi telah memenuhi standar minimal sebagaimana dimaksud dalam POJK SPTI;
   (b) operasional Teknologi Informasi, untuk memastikan kesesuaian pelaksanaan penyelenggaraan Teknologi Informasi dengan kebijakan dan prosedur;
   (c) jaringan komunikasi, untuk memastikan pengelolaan jaringan komunikasi telah sesuai dengan kebijakan dan prosedur;
   (d) pengamanan informasi, untuk memastikan pemenuhan pengamanan fisik dan pengamanan *logic* dalam penyelenggaraan Teknologi Informasi;
   (e) rencana pemulihan bencana, untuk memastikan rencana pemulihan bencana dapat dijalankan setiap saat; dan
   (f) fungsionalitas dari seluruh perangkat Teknologi Informasi yang digunakan, untuk menjamin terpenuhinya unsur kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dalam operasional BPR atau BPRS.

f) prosedur audit intern terhadap penyelenggaraan Teknologi Informasi untuk setiap aktivitas Teknologi Informasi dalam penyelenggaraan Teknologi Informasi yang memerlukan audit.

2. Perencanaan Audit

Organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi harus memiliki rencana audit tahunan terkait penyelenggaraan Teknologi Informasi baik terhadap satuan kerja Teknologi Informasi maupun satuan kerja yang bertanggung jawab terhadap penyelenggaraan Teknologi

Informasi. Dalam melakukan fungsi audit intern untuk menilai penyelenggaraan Teknologi Informasi, organ pelaksana fungsi audit intern paling sedikit melakukan hal-hal sebagai berikut:

(a) mengidentifikasi data, aplikasi dan sistem operasi, teknologi, fasilitas dan personil; dan
(b) mengidentifikasi kegiatan dan proses bisnis yang menggunakan Teknologi Informasi.

Rencana audit intern terhadap penyelenggaraan Teknologi Informasi harus mendapat persetujuan dari Direksi.

3. Pelaksanaan Audit

Dalam rangka melaksanakan rencana tahunan audit, program audit (*audit working plan* yang selanjutnya disebut "AWP") disusun untuk setiap penugasan audit, yang paling sedikit 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; dan
(d) langkah-langkah teknis audit yang diperlukan untuk mencapai tujuan audit.

Dalam pelaksanaannya, audit intern terhadap penyelenggaraan Teknologi Informasi harus memperhatikan aspek-aspek kerahasiaan terhadap data dan informasi yang diperoleh. Organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi harus memperhatikan fleksibilitas AWP agar dapat disesuaikan dan dilengkapi sesuai dengan risiko yang diidentifikasi.

Dalam pelaksanaan audit dilengkapi dengan kertas kerja, isi dan format laporan hasil audit, dokumentasi dan distribusi, serta pemantauan tindak lanjutnya. Temuan audit harus disertai dengan bukti-bukti dan kertas kerja pemeriksaan yang didokumentasikan dengan baik.

4. Pelaporan

Laporan pelaksanaan fungsi audit intern terhadap penyelenggaraan Teknologi Informasi merupakan sarana bagi Direksi untuk membantu melakukan penilaian terhadap kualitas

dan kinerja satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi, serta memberikan saran perbaikan. Laporan tersebut disampaikan secara tepat waktu kepada Direktur Utama dan Dewan Komisaris, dengan tembusan disampaikan kepada anggota Direksi yang membawahkan fungsi kepatuhan dan satuan kerja yang diaudit. Laporan mengenai pelaksanaan fungsi audit intern terhadap penyelenggaraan Teknologi Informasi disampaikan juga kepada Otoritas Jasa Keuangan sebagai bagian dari laporan pelaksanaan dan pokok-pokok hasil audit intern atau disampaikan secara terpisah sesuai dengan ketentuan dan Peraturan Otoritas Jasa Keuangan.

5. Tindak Lanjut Audit

   Auditee harus memberikan tanggapan terhadap hasil audit. Apabila temuan perlu ditindaklanjuti, *auditee* harus memberikan komitmen dan target waktu penyelesaiannya. Selanjutnya, organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi harus memantau pelaksanaan komitmen *auditee* atas hasil audit secara berkala dan melakukan verifikasi terhadap perbaikan yang telah dilakukan.

   Organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi harus memelihara dokumentasi atas hasil tindak lanjut tersebut. Laporan tindak lanjut hasil audit disampaikan kepada Direktur Utama dan Dewan Komisaris dengan tembusan kepada anggota Direksi yang membawahkan fungsi kepatuhan.

6. Pengembangan dan Pengujian Sistem Elektronik

   Organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi perlu berperan dalam pengembangan Sistem Elektronik untuk memastikan bahwa Sistem Elektronik sesuai dengan kebutuhan BPR atau BPRS serta ketentuan yang berlaku, memiliki kontrol yang memadai, dan memiliki sarana untuk penelusuran kembali (jejak audit), namun tidak dapat berperan sebagai penentu Sistem Elektronik diimplementasikan, melainkan berpartisipasi sebagai nara sumber dalam aspek pengendalian khususnya mengenai standar pengamanan yang

diperlukan. Peran ini diperlukan agar auditor dapat menjaga independensi dan obyektifitas dalam audit yang dilakukan apabila Sistem Elektronik diimplementasikan. Selain itu organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi dapat memberikan rekomendasi kepada Direktur Utama atau anggota Direksi lainnya mengenai kontrol yang perlu diterapkan.

C. PELAKSANAAN FUNGSI AUDIT INTERN TERHADAP PENYELENGGARAAN TEKNOLOGI INFORMASI YANG DILAKSANAKAN OLEH AUDITOR EKSTERN

Dalam hal terdapat keterbatasan kemampuan fungsi audit intern terhadap Teknologi Informasi BPR atau BPRS, pelaksanaan fungsi audit intern dapat dilakukan oleh auditor ekstern seperti Kantor Akuntan Publik atau Lembaga Audit Teknologi Informasi Independen. Penggunaan jasa auditor ekstern untuk melaksanakan fungsi audit intern terhadap penyelenggaraan Teknologi Informasi BPR atau BPRS tidak mengurangi tanggung jawab organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi atas temuan audit dan tindak lanjutnya.

Penggunaan jasa auditor ekstern tersebut harus mempertimbangkan ukuran dan kompleksitas usaha BPR atau BPRS. Pelaksanaan fungsi audit intern terhadap penyelenggaraan Teknologi Informasi oleh auditor ekstern tetap memperhatikan aspek kompetensi antara lain pengetahuan dan pengalaman yang memadai dan independensi serta didasari perjanjian kerja sama. Meskipun pelaksanaan fungsi audit intern dilakukan oleh auditor ekstern, prosedur audit terhadap penyelenggaraan Teknologi Informasi harus tetap mengacu pada kebijakan dan prosedur audit intern terhadap penyelenggaraan Teknologi Informasi yang dimiliki oleh BPR atau BPRS.

D. AUDIT INTERN TERHADAP AKTIVITAS YANG DISELENGGARAKAN OLEH PENYEDIA JASA TEKNOLOGI INFORMASI

Pihak yang melaksanakan fungsi audit intern BPR dan BPRS harus memastikan pengendalian yang dioperasikan oleh penyedia jasa

Teknologi Informasi dan melakukan pengujian atas efektivitas pengendalian tersebut. BPR dan BPRS harus memastikan bahwa perjanjian dengan pihak penyedia jasa Teknologi Informasi mencakup klausul penyediaan hak akses baik secara *logic* maupun fisik bagi:

1. auditor intern BPR dan BPRS;
2. auditor ekstern yang ditunjuk oleh BPR dan BPRS; dan
3. Otoritas Jasa Keuangan,

untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan, serta menyatakan tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-perundangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan.

BAB VIII

KERJA SAMA DENGAN PENYEDIA JASA TEKNOLOGI INFORMASI

Dalam rangka meningkatkan efektivitas dan efisiensi untuk mencapai tujuan strategis, BPR dan BPRS dapat melakukan kerja sama dengan penyedia jasa Teknologi Informasi. Kerja sama tersebut menyebabkan BPR dan BPRS memiliki ketergantungan terhadap jasa yang diberikan secara berkesinambungan dan/atau dalam periode tertentu.

Kerja sama dengan penyedia jasa Teknologi Informasi dapat mempengaruhi risiko BPR dan BPRS antara lain risiko operasional, kepatuhan, dan reputasi. Risiko tersebut dapat disebabkan antara lain karena adanya kegagalan penyedia jasa Teknologi Informasi dalam menyediakan jasa, pelanggaran terhadap pengamanan, atau ketidakmampuan untuk mematuhi ketentuan dan peraturan perundang-undangan. BPR dan BPRS tetap wajib bertanggung jawab terhadap penyelenggaraan Teknologi Informasi yang dilakukan bekerjasama dengan penyedia jasa Teknologi Informasi.

A. PROSES PEMILIHAN PENYEDIA JASA TEKNOLOGI INFORMASI

1. Penetapan Kebutuhan

   Dalam hal BPR dan BPRS akan melakukan kerja sama dengan penyedia jasa Teknologi Informasi, BPR dan BPRS perlu melakukan penetapan kebutuhan dengan mempertimbangkan paling sedikit:

   a) hasil identifikasi fungsi atau aktivitas spesifik yang penyelenggaraannya akan dilaksanakan oleh penyedia jasa Teknologi Informasi; dan
   b) hasil penilaian terhadap risiko yang dapat timbul akibat kerja sama yang akan dilaksanakan,

   Tahap penetapan kebutuhan tersebut harus menghasilkan suatu dokumen yang berisi secara rinci mengenai kebutuhan BPR atau BPRS terhadap jasa yang akan disediakan oleh penyedia jasa Teknologi Informasi. Isi dari dokumen tersebut paling sedikit mencakup:

a) lingkup dan karakteristik dari layanan, teknologi yang digunakan, dan dukungan kepada nasabah;
b) standar dan tingkat layanan meliputi ketersediaan dan kinerja, manajemen perubahan, kualitas layanan, keamanan, dan kelangsungan usaha;
c) karakteristik minimal yang harus dipenuhi oleh penyedia jasa Teknologi Informasi yang akan digunakan seperti pengalaman, *process control*, kondisi keuangan, dan referensi mengenai reputasi;
d) teknis pemantauan yang dilakukan oleh BPR atau BPRS dan kriteria pelaporan yang dilakukan oleh penyedia jasa Teknologi Informasi;
e) persyaratan yang harus dipenuhi antara lain terkait dengan sistem, data, maupun pelatihan personel, pada saat BPR atau BPRS melakukan transisi atau migrasi ke sistem yang disediakan oleh penyedia jasa Teknologi Informasi;
f) jangka waktu perjanjian kerja sama, penghentian, dan cakupan minimal dari perjanjian kerja sama; dan
g) perlindungan perjanjian kerja sama seperti pembatasan kewajiban, ganti rugi, dan asuransi.

Dalam hal penyelenggaraan Teknologi Informasi dipertimbangkan untuk dilakukan oleh pihak terkait BPR atau BPRS, Direksi BPR atau BPRS harus memastikan bahwa persiapan dan proses pelaksanaan yang dilakukan tidak berbeda dalam hal penyelenggaraan Teknologi Informasi dilakukan oleh pihak tidak terkait BPR atau BPRS (*arm's length principle*).

2. Analisis Biaya dan Manfaat

Setelah penetapan kebutuhan atas kerja sama yang akan dilakukan oleh BPR atau BPRS dengan penyedia jasa Teknologi Informasi, BPR dan BPRS harus melakukan analisis terhadap biaya langsung maupun tidak langsung dalam penawaran tertulis oleh penyedia jasa Teknologi Informasi dengan spesifikasi sesuai kebutuhan, jenis layanan, hal-hal yang diperlukan dalam menentukan efektivitas biaya, jangka waktu penyelesaian, pengamanan dan kelangsungan bisnis, SLA, serta solusi untuk masalah yang dihadapi.

Pada saat BPR dan BPRS melakukan analisis penawaran tertulis yang diajukan, terdapat kemungkinan ditemukannya ketidaksesuaian dengan kebutuhan BPR atau BPRS. Oleh karena itu, BPR dan BPRS harus mengevaluasi perbedaan tersebut dan dampaknya terhadap sasaran dan jasa yang diharapkan BPR atau BPRS.

Dalam rangka mengoptimalkan proses analisis biaya dan manfaat, selain menggunakan harga perkiraan sendiri (*owners estimate*), BPR dan BPRS dapat melakukan perbandingan biaya dan manfaat yang ditawarkan antara penyedia jasa Teknologi Informasi. Selanjutnya apabila penawaran tertulis tersebut telah memenuhi kebutuhan atau sesuai spesifikasi kebutuhan yang telah dibuat BPR atau BPRS, BPR dan BPRS perlu melakukan negosiasi dengan penyedia jasa Teknologi Informasi sebelum pembuatan perjanjian kerja sama.

3. Uji Tuntas (*Due Diligence*) terhadap Penyedia Jasa Teknologi Informasi

Uji tuntas terhadap penyedia jasa Teknologi Informasi dilakukan dalam rangka mendapatkan keyakinan bahwa penyedia jasa Teknologi Informasi mampu memenuhi kebutuhan BPR atau BPRS. Untuk mendapatkan keyakinan dimaksud, BPR dan BPRS dapat melakukan evaluasi dan menilai informasi yang terkait dengan penyedia jasa Teknologi Informasi antara lain meliputi:

a) eksistensi dan riwayat penyedia jasa Teknologi Informasi;
b) kualifikasi, latar belakang, dan reputasi pemilik penyedia jasa Teknologi Informasi;
c) perusahaan lain yang menggunakan jasa yang sama dari penyedia jasa Teknologi Informasi sebagai referensi;
d) kondisi keuangan termasuk pemeriksaan atas laporan keuangan yang telah diaudit;
e) kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual;
f) teknologi dan arsitektur sistem;
g) lingkungan pengendalian intern, riwayat pengamanan, dan cakupan audit;
h) kepatuhan terhadap peraturan perundang-undangan;

i) kepercayaan dan keberhasilan dalam melakukan hubungan dengan sub kontraktor;
j) asuransi dan jaminan pemeliharaan;
k) kemampuan untuk menyediakan pemulihan bencana dan keberlangsungan usaha (*business continuity*);
l) penerapan manajemen risiko; dan/atau
m) laporan hasil audit pihak independen.

Uji tuntas terhadap penyedia jasa Teknologi Informasi yang dilakukan BPR atau BPRS selama proses pemilihan harus didokumentasikan dengan baik dan dilakukan secara berkala sebagai bagian dari proses pemantauan dan kontrol. Dalam melakukan uji tuntas secara berkala terhadap penyedia jasa Teknologi Informasi sebaiknya BPR dan BPRS memperhatikan perubahan atau perkembangan yang ada selama kurun waktu sejak uji tuntas terakhir dengan menggunakan informasi terkini.

4. Penentuan Penyedia Jasa Teknologi Informasi

Dalam menentukan penyedia jasa Teknologi Informasi yang dipilih untuk digunakan oleh BPR atau BPRS dalam menyelenggarakan Teknologi Informasi, BPR dan BPRS harus memperhatikan hal-hal sebagai berikut:

a) laporan-laporan yang pernah dibuat yang mencerminkan kinerja penyedia jasa Teknologi Informasi sebelumnya yang diperlukan untuk menilai kinerja penyedia jasa Teknologi Informasi telah memadai;
b) kemampuan menyampaikan laporan yang mencerminkan kinerja penyedia jasa Teknologi Informasi yang diperlukan untuk memantau bahwa kinerja penyedia jasa Teknologi Informasi memadai;
c) hasil analisis terhadap biaya dan manfaat dari setiap pilihan penyedia jasa Teknologi Informasi yang akan dipilih dan analisis terhadap pemenuhan jangka waktu penggunaan jasa sesuai dengan rencana bisnis BPR atau BPRS;
d) penerapan prinsip pengendalian Teknologi Informasi secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen terhadap penyedia jasa Teknologi Informasi, termasuk pengamanan *logic* dan fisik;

e) informasi dari berbagai sumber termasuk laporan tahunan penyedia jasa Teknologi Informasi dalam rangka mengevaluasi keandalan, kinerja, reputasi, dan kelangsungan penyediaan layanan dari penyedia jasa Teknologi Informasi;

f) ketersediaan akses terhadap Pangkalan Data bagi Otoritas Jasa Keuangan, auditor intern, auditor ekstern yang ditunjuk oleh BPR dan BPRS, serta pihak lain yang berwenang sesuai dengan peraturan perundang-undangan, dalam hal memerlukan data terkini maupun data yang telah lalu;

g) dokumen penyeleksian yang memuat pertimbangan mengenai penerapan "hubungan kerja sama secara wajar (*arm's length principle*)", dalam hal penyedia jasa Teknologi Informasi merupakan pihak terkait BPR atau BPRS.

B. PERJANJIAN KERJA SAMA DENGAN PENYEDIA JASA TEKNOLOGI INFORMASI

Perjanjian kerja sama penyelenggaraan Teknologi Informasi dengan penyedia jasa Teknologi Informasi paling sedikit mencakup:

1. cakupan pekerjaan/jasa;
2. biaya dan jangka waktu perjanjian kerja sama;
3. batasan risiko yang ditanggung oleh BPR atau BPRS dan penyedia jasa Teknologi Informasi yang diakibatkan perubahan antara lain:
   a) ruang lingkup perjanjian kerja sama;
   b) ruang lingkup bisnis dan organisasi perusahaan penyedia jasa Teknologi Informasi; dan
   c) aspek hukum antara lain regulasi, hak cipta, paten, dan *trade mark*;
4. larangan bagi penyedia jasa Teknologi Informasi untuk menggunakan atau mengungkapkan informasi yang dimiliki BPR dan BPRS tanpa persetujuan BPR atau BPRS;
5. jaminan dari penyedia jasa Teknologi Informasi untuk pengamanan dan kerahasiaan data terutama rahasia bank dan data pribadi nasabah termasuk bahwa Sistem Elektronik hanya

bisa diakses oleh pemilik data (BPR dan BPRS) serta Sistem Elektronik tersebut tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam Sistem Elektronik dan data BPR atau BPRS;

6. pernyataan bahwa penyedia jasa Teknologi Informasi memberikan jaminan keandalan Sistem Elektronik, termasuk tidak menggunakan fitur Sistem Elektronik yang dapat mengakibatkan Sistem Elektronik tersebut tidak berfungsi dengan baik;
7. standar spesifikasi dan kinerja Sistem Elektronik paling sedikit mencakup:
   a) kinerja dan fungsional yang diharapkan dari Sistem Elektronik;
   b) persyaratan dan infrastruktur yang diperlukan untuk menjalankan Sistem Elektronik;
   c) identifikasi kebutuhan uji coba guna menentukan pemenuhan standar kinerja Sistem Elektronik; dan
   d) tindakan yang harus dilakukan penyedia jasa Teknologi Informasi apabila Sistem Elektronik gagal pada saat uji coba.
8. kesediaan penyedia jasa Teknologi Informasi untuk memberikan dokumen teknis kepada BPR atau BPRS terkait dengan jasa yang dikerjakan oleh penyedia jasa Teknologi Informasi antara lain alur proses Teknologi Informasi, petunjuk pelaksanaan (*manual book*), struktur Pangkalan Data, dan aplikasi *online help* pada Sistem Elektronik yang bekerja secara interaktif;
9. jaminan ketersediaan akses ke kode sumber dalam hal:
   a) penyedia jasa Teknologi Informasi tidak dapat memberikan layanan lagi;
   b) diperlukan modifikasi yang tidak dapat dilakukan oleh pihak penyedia jasa Teknologi Informasi; dan/atau
   c) perangkat lunak dinilai penting untuk kelangsungan operasional BPR atau BPRS.
10. kesediaan penyedia jasa Teknologi Informasi membantu proses konversi perangkat lunak termasuk data dan format data pada saat penggantian sistem diperlukan di masa mendatang;

11. penyedia jasa Teknologi Informasi memberikan jaminan paling sedikit bahwa Sistem Elektronik:
    a) tidak melanggar hak kekayaan intelektual dari pihak lain;
    b) tidak mengandung kode rahasia atau pembatasan secara otomatis yang tidak diungkapkan pada perjanjian;
    c) bekerja sesuai dengan spesifikasi dan penyedia jasa Teknologi Informasi bertanggung jawab dalam hal terjadi permasalahan; dan
    d) dijamin pemeliharaannya oleh penyedia jasa Teknologi Informasi selama jangka waktu perjanjian.
12. SLA yang memuat standar kinerja dari penyedia jasa Teknologi Informasi antara lain mengenai tingkat pelayanan yang diperjanjikan (*service levels*) dan target kinerja;
13. klausula bahwa SLA tetap berlaku dalam hal terjadi perubahan kepemilikan baik pada BPR atau BPRS maupun penyedia jasa Teknologi Informasi;
14. laporan hasil pemantauan kinerja penyedia jasa Teknologi Informasi yang terkait dengan SLA;
15. penyedia jasa Teknologi Informasi tidak dapat memodifikasi Sistem Elektronik yang telah disepakati dalam perjanjian tanpa persetujuan dari kedua belah pihak;
16. kewajiban penyedia jasa Teknologi Informasi untuk melaporkan setiap kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan Teknologi Informasi yang dapat atau telah mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelangsungan operasional BPR atau BPRS;
17. keharusan penyedia jasa Teknologi Informasi untuk melakukan *transfer of knowledge* kepada BPR atau BPRS dengan merencanakan pelatihan terhadap sumber daya manusia BPR atau BPRS, antara lain mengenai jumlah sumber daya manusia yang dilatih, bentuk pelatihan, dan biaya yang diperlukan, yang bertujuan agar sumber daya manusia BPR atau BPRS memahami Teknologi Informasi yang digunakan terutama alur proses Teknologi Informasi dan struktur Pangkalan Data dari Sistem Elektronik yang disediakan oleh penyedia jasa Teknologi Informasi tersebut;

18. sanksi dan/atau penalti terhadap pembatalan dan/atau pelanggaran perjanjian kerja sama;
19. kepatuhan pada ketentuan dan peraturan perundang-undangan termasuk penyelesaian sengketa dalam hal terjadi perselisihan;
20. jaminan bahwa Penyedia jasa Teknologi Informasi menerapkan prinsip pengendalian Teknologi Informasi secara memadai yang dibuktikan dengan hasil audit oleh pihak independen;
21. tanggung jawab terus menerus dari penyedia jasa Teknologi Informasi untuk menjaga keamanan dan kerahasiaan data/informasi BPR atau BPRS;
22. kepemilikan dan hak cipta (*license*);
23. jaminan bahwa penyedia jasa Teknologi Informasi tetap mendukung jasa yang diberikan kepada BPR atau BPRS selama jangka waktu tertentu setelah implementasi;
24. larangan melakukan pengalihan (subkontrak) sebagian atau seluruh kegiatan penyelenggaraan Teknologi Informasi BPR atau BPRS kepada penyedia jasa Teknologi Informasi lain;
25. ketersediaan sarana komunikasi *online*, pengamanan terhadap akses dan transmisi data dari dan ke Pusat Data serta Pusat Pemulihan Bencana, dan penyelenggaraan Teknologi Informasi lainnya sesuai dengan ketentuan peraturan perundang-undangan;
26. pengaturan yang jelas mengenai rekam cadang, *contingency*, *record protection* termasuk perangkat keras, perangkat lunak, dan *data files*, untuk menjamin kelangsungan penyelenggaraan Teknologi Informasi;
27. pengaturan mengenai pengamanan dalam pengiriman dokumen yang diperlukan dari dan ke Pusat Data serta Pusat Pemulihan Bencana, dan penyelenggaraan Teknologi Informasi lainnya sesuai dengan ketentuan peraturan perundang-undangan;
28. pernyataan tidak keberatan dalam hal Otoritas Jasa Keuangan atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-undangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan;
29. ketersediaan data dan informasi untuk keperluan pemeriksaan sebagaimana dimaksud pada angka 28, termasuk hak akses, baik secara *logic* maupun fisik terhadap Sistem Elektronik yang

diselenggarakan termasuk data yang dikelola oleh penyedia jasa Teknologi Informasi;

30. tanggung jawab penyedia jasa Teknologi Informasi dalam menyediakan tenaga ahli yang didukung dengan sertifikat keahlian sesuai dengan keperluan penyelenggaraan Teknologi Informasi;
31. kemungkinan menghentikan, mengubah, membuat perjanjian baru, atau mengambil alih kegiatan yang diselenggarakan oleh penyedia jasa Teknologi Informasi, serta mengakhiri perjanjian sebelum jangka waktu berakhirnya perjanjian, termasuk dalam hal ini atas permintaan Otoritas Jasa Keuangan; dan
32. kewajiban penyedia jasa Teknologi Informasi untuk menyediakan Rencana Pemulihan Bencana yang teruji dan memadai.

C. TINDAK LANJUT ATAS REALISASI PERJANJIAN KERJA SAMA DENGAN PENYEDIA JASA TEKNOLOGI INFORMASI

1. Antisipasi Risiko

Dalam hal kerja sama dengan penyedia jasa Teknologi Informasi telah direalisasikan, BPR dan BPRS harus mengantisipasi risiko dari penyelenggaraan Teknologi Informasi yang diserahkan kepada penyedia jasa Teknologi Informasi. Dalam rangka mengantisipasi risiko tersebut, BPR dan BPRS melakukan pemantauan untuk mengetahui secara dini apabila terdapat kondisi sebagai berikut:

a) memburuknya kinerja penyelenggaraan Teknologi Informasi BPR dan BPRS yang disebabkan oleh penyedia jasa Teknologi Informasi yang dapat berdampak signifikan terhadap kegiatan usaha BPR atau BPRS;
b) penyedia jasa Teknologi Informasi mengalami kesulitan keuangan yang menyebabkan insolven, dalam proses menuju likuidasi, atau dinyatakan pailit berdasarkan keputusan pengadilan;
c) terdapat pelanggaran oleh penyedia jasa Teknologi Informasi terhadap kewajiban menjaga keamanan data dan informasi termasuk rahasia bank dan data pribadi nasabah; dan/atau

d) terdapat kondisi yang menyebabkan BPR atau BPRS tidak dapat menyediakan data dan informasi yang diperlukan dalam rangka pengawasan oleh Otoritas Jasa Keuangan.

2. Tindak Lanjut Risiko

Dalam hal BPR dan BPRS menemukan kondisi sebagaimana dimaksud pada angka 1. di atas, BPR dan BPRS wajib melakukan tindakan tertentu paling sedikit:

a) melaporkan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) hari kerja sejak kondisi tersebut di atas diketahui oleh BPR atau BPRS;
b) memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian kerja sama dengan penyedia jasa Teknologi Informasi apabila diperlukan; dan
c) melaporkan kepada Otoritas Jasa Keuangan mengenai keputusan tindak lanjut yang telah dan/atau akan diambil, paling lambat 10 (sepuluh) hari kerja sejak tanggal laporan kondisi sebagaimana dimaksud dalam huruf a).

3. Rencana Darurat

Dalam hal dilakukan penghentian kerja sama sebagaimana dimaksud pada angka 2 huruf b) atau atas perintah Otoritas Jasa Keuangan sebelum berakhirnya jangka waktu perjanjian kerja sama, BPR dan BPRS harus memiliki rencana darurat (*contingency plan*) dalam rangka menjaga kelangsungan usaha BPR atau BPRS.

4. Rencana Pemulihan Bencana

BPR dan BPRS harus memastikan bahwa ketergantungan pada penyedia jasa Teknologi Informasi dapat dimitigasi sehingga BPR dan BPRS tetap mampu menyelenggarakan Teknologi Informasi dalam hal terjadi bencana, dengan cara:

a) memastikan bahwa penyedia jasa Teknologi Informasi memiliki Rencana Pemulihan Bencana sesuai dengan jenis, cakupan, dan kompleksitas aktivitas/jasa Teknologi Informasi yang diberikan; dan
b) secara aktif mendapatkan jaminan kesiapan Rencana

Pemulihan Bencana milik penyedia jasa Teknologi Informasi seperti pengujian secara berkala atas Rencana Pemulihan Bencana.

5. Jaminan Keberlangsungan Penyelenggaraan Teknologi Informasi

Dalam rangka menjaga keberlangsungan penyelenggaraan Teknologi Informasi, BPR dan BPRS perlu melakukan mitigasi terhadap ketergantungan pada penyedia jasa Teknologi Informasi, antara lain:

a) memastikan ketersediaan kode sumber oleh penyedia jasa Teknologi Informasi pada saat diperlukan, dengan cara:
   1) menyerahkan kode sumber kepada BPR atau BPRS; atau
   2) dalam hal penyedia jasa Teknologi Informasi tidak menyerahkan kode sumber kepada BPR atau BPRS, penyedia jasa Teknologi Informasi menempatkan kode sumber pada pihak ketiga yang terpercaya yang dapat menjamin penyerahan kode sumber kepada BPR atau BPRS.

b) penyedia jasa Teknologi Informasi harus memberikan jaminan kepada BPR dan BPRS bahwa kelangsungan aplikasi didukung oleh *principal* pengembang perangkat lunak, dalam hal kode sumber tidak dimiliki oleh penyedia jasa Teknologi Informasi;

Glosarium

1. **Akses (*Access*):**
   kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan

2. ***Administrator Log*:**
   file di komputer yang menyimpan informasi mengenai kegiatan administrator.

3. ***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.

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

5. **Rekam Jejak Audit (*Audit Trail*):**
   file di komputer yang menyimpan informasi mengenai kegiatan pengguna atau komputer yang tersimpan secara kronologis, yang dapat digunakan untuk audit atau penelusuran.

6. ***Authentication*:**
   kemampuan dari setiap pihak dalam transaksi untuk menguji kebenaran dari pihak lain.

7. ***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.

8. **Rekam Cadang (*Back Up*):**
   salinan dari dokumen asli atau cadangan dari mesin utama yang dapat digunakan apabila terjadi gangguan pada mesin utama. Rekam cadang dapat berupa rekam cadang data maupun rekam cadang *system.* Rekam cadang dapat ditempatkan secara *on site* di lokasi Pusat Data dan atau *off site* di lokasi alternatif.

9. ***Biometric Device:***
perangkat atau sistem teknologi pengamanan informasi yang menggunakan bagian tubuh sebagai identitas dan otentikasi.

10. ***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 pemangku kepentingan.

11. ***Business Continuity Plan*** **(BCP):**
suatu rangkaian proses yang dilakukan untuk memastikan terus berlangsungnya kegiatan dalam kondisi mendapatkan gangguan atau bencana.

12. ***Client*****:**
komputer dalam jaringan yang menggunakan sumber daya yang disediakan oleh peladen (*server*).

13. ***Contigency 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.

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

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

16. **Pusat Data (*Data Center*):**
suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

17. ***Denial of Service*** **(DoS):**
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, gangggguan pada peladen (*server*) serta gangguan penyediaan jasa kepada sistem lain atau pengguna.

18. **Tanda Tangan Elektronik *(Digital signatures)*:**
tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

19. **Rencana Pemulihan Bencana (*Disaster Recovery Plan*):**
dokumen yang berisikan rencana dan langkah- langkah memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar BPR dan BPRS dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana.

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

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

22. ***Downtime*:**
lamanya sistem tidak dapat berfungsi dan digunakan oleh pengguna karena adanya gangguan *hardware, software* dan komunikasi.

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

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

25. ***Firewall*:**
peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian 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.

26. *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.

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

28. *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.*

29. *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.

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

31. *Interoperability*:
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).

32. *System Integration Testing*:
pengujian terhadap keseluruhan fungsional terhadap Sistem setelah diintegrasikan menjadi satu kesatuan yang utuh.

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

34. *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.

35. *Mobile Banking*:
layanan yang memungkinkan nasabah BPR atau BPRS melakukan transaksi perbankan melalui *handphone*. *Mobile banking* umumnya dilakukan melalui sms atau *mobile internet* namun dapat juga menggunakan program khusus yang di unduh melalui *handphone*.

36. Nirsangkal (*Non-repudiation*):
suatu cara untuk memastikan kebenaran pengirim dan penerima sehingga tidak ada pihak yang dapat menyangkal.

37. *Off-line*:
sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

38. Alih Daya (*Outsourcing*):
penggunaan pihak lain (ekstern) dalam penyelenggaraan teknologi informasi BPR atau BPRS yang menyebabkan BPR atau BPRS memiliki ketergantungan terhadap jasa yang diberikan pihak lain tersebut secara berkesinambungan dan atau dalam periode tertentu.

39. *Parallel Run*:
merupakan salah satu strategi implementasi sistem di mana kedua sistem lama dan baru berjalan berdampingan sampai pengguna yakin bahwa sistem baru tidak memiliki masalah. Setelah periode waktu ketika sistem baru terbukti bekerja dengan benar, sistem lama akan dihapus sepenuhnya dan pengguna akan tergantung hanya pada sistem baru.

40. *Password*:
angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.

41. *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.

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

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

44. Pengamanan *Logic*:
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.

45. *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,* dan lain-lain.

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

47. *Super User*:
user id yang memiliki kewenangan sangat luas.

48. *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).*

49. *Proprietary*:
jenis kepemilikan secara eksklusif oleh pihak tertentu yang diperoleh secara legal.

50. *Public Key Infrastructure*:
suatu pengolahan/pengaturan dimana suatu pihak ketiga yang dapat dipercaya menyediakan pemeriksaan secara seksama dan memastikan keabsahan suatu identitas.

51. *Quality Assurance*:
aktivitas yang memastikan produk atau jasa memenuhi standar yang ditetapkan termasuk keandalan, kegunaan, kinerja dan standar kualitas umum yang ditetapkan oleh perusahaan.

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

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

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

55. *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.

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

57. Kode Sumber (*Source Code*):
suatu rangkaian perintah, pernyataan, dan/atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dapat dibaca dan dipahami orang.

58. *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.

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

60. *Stress Testing*:
uji ketahanan terhadap kemampuan Sistem Elektronik atau Aplikasi Inti Perbankan dalam menangani proses atau transaksi dalam skala/jumlah yang besar.

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

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

63. *System Development Life Cycle (SDLC)*:
siklus pengembangan sistem yang meliputi langkah-langkah paling sedikit sebagai berikut: (1) *system planning*, (2) *system analysis*, (3) *system design*, (4) *system selection*, (5*) system implementation*, (6) *system maintenance,* dan *(7) system disposal*.

64. *System Log*:
file di komputer yang menyimpan informasi mengenai kegiatan sistem atau komputer.

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

66. *Trojan Horse*:
program yang bersifat merusak yang disusupkan oleh peretas (*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*".

67. *Unit Testing*:
uji coba atas fungsional setiap unit atau sub modul dari sistem yang telah selesai dikembangkan.

68. *Uninterruptible Power Supply* (UPS):
perangkat yang mempunyai fungsi utama sebagai penyedia listrik cadangan dengan jangka waktu tertentu bagi perangkat elektronik yang terpasang.

69. *Upload* dan *Download*:
transfer data elektronik antara dua komputer atau sistem yang sejenis.

70. *User Acceptance Test*:
uji coba akhir yang dilakukan oleh pengguna akhir terhadap Sistem yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem apakah telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan.

71. *User Log*:
file di komputer yang menyimpan informasi mengenai kegiatan user seperti waktu *login* dan *logout*

72. 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 *attachment* surat elektronik, *game*, program bajakan, dan lain-lain.

73. *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 smartphone.

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

Ditetapkan di Jakarta
pada tanggal 6 April 2017

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,
ttd
NELSON TAMPUBOLON

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana