OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA

SALINAN

PERATURAN OTORITAS JASA KEUANGAN

NOMOR 38 /POJK.03/2016

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM
PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DENGAN RAHMAT TUHAN YANG MAHA ESA

DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Menimbang : a. bahwa perkembangan teknologi informasi dapat dimanfaatkan oleh bank untuk meningkatkan efisiensi kegiatan operasional dan mutu pelayanan bank kepada nasabah;

b. bahwa penggunaan teknologi informasi dalam kegiatan operasional bank juga dapat meningkatkan risiko yang dihadapi bank;

c. bahwa dengan semakin meningkatnya risiko yang dihadapi, bank perlu menerapkan manajemen risiko secara efektif;

d. bahwa teknologi informasi merupakan aset yang berharga bagi bank sehingga pengelolaannya bukan hanya merupakan tanggung jawab unit kerja penyelenggara teknologi informasi namun juga seluruh pihak yang menggunakan;

e. bahwa dalam rangka implementasi kerangka Basel (*Basel framework*) diperlukan infrastruktur teknologi informasi yang memadai;

f. bahwa sejalan dengan dinamika pengaturan yang terkait dengan penggunaan teknologi informasi serta perkembangan standar nasional dan internasional, perlu dilakukan penyempurnaan ketentuan mengenai penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank;

g. bahwa sehubungan dengan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f perlu menetapkan Peraturan Otoritas Jasa Keuangan tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum;

Mengingat : 1. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (Lembaran Negara Tahun 1992 Nomor 31, Tambahan Lembaran Negara Nomor 3472) sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 (Lembaran Negara Tahun 1998 Nomor 182, Tambahan Lembaran Negara Nomor 3790);

2. Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 94, Tambahan Lembaran Negara Republik Indonesia Nomor 4867);

3. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253);

MEMUTUSKAN:

Menetapkan : PERATURAN OTORITAS JASA KEUANGAN TENTANG PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Otoritas Jasa Keuangan ini yang dimaksud dengan:

1. Bank adalah Bank Umum sebagaimana dimaksud dalam Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998, termasuk kantor cabang dari bank yang berkedudukan di luar negeri, dan Bank Umum Syariah serta Unit Usaha Syariah sebagaimana dimaksud dalam Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah.
2. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
3. Layanan Perbankan Elektronik (*Electronic Banking*) adalah layanan bagi nasabah Bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik.
4. Rencana Strategis Teknologi Informasi (*Information Technology Strategic Plan*) adalah dokumen yang menggambarkan visi dan misi Teknologi Informasi Bank, strategi yang mendukung visi dan misi Teknologi Informasi Bank, dan prinsip-prinsip utama yang menjadi acuan dalam penggunaan Teknologi Informasi untuk memenuhi kebutuhan bisnis serta mendukung rencana strategis jangka panjang.
5. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
6. Pusat Data (*Data Center*) adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik

dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

7. Pusat Pemulihan Bencana (*Disaster Recovery Center*) adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia.
8. Pangkalan Data (*Database*) adalah sekumpulan data komprehensif dan disusun secara sistematis, dapat diakses oleh pengguna sesuai wewenang masing-masing, dan dikelola oleh administrator Pangkalan Data (*Database administrator*).
9. Rencana Pemulihan Bencana (*Disaster Recovery Plan*) adalah dokumen yang berisikan rencana dan langkah-langkah untuk menggantikan dan/atau memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar Bank dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana.
10. Pemrosesan Transaksi Berbasis Teknologi Informasi adalah kegiatan berupa penambahan, perubahan, penghapusan, dan/atau otorisasi data yang dilakukan pada sistem aplikasi yang digunakan untuk memproses transaksi.
11. Direksi:
    a) bagi Bank berbentuk badan hukum Perseroan Terbatas adalah direksi sebagaimana dimaksud dalam Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas;
    b) bagi Bank berbentuk badan hukum:
        1) Perusahaan Umum Daerah atau Perusahaan Perseroan Daerah adalah direksi sebagaimana dimaksud dalam Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah

diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015;

2) Perusahaan Daerah adalah direksi bagi Bank yang belum berubah bentuk menjadi Perusahaan Umum Daerah atau Perusahaan Perseroan Daerah sebagaimana dimaksud Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015;

c) bagi Bank berbentuk badan hukum Koperasi adalah pengurus sebagaimana dimaksud dalam Undang-Undang Nomor 25 Tahun 1992 tentang Perkoperasian;

d) bagi Bank yang berstatus sebagai kantor cabang dari bank yang berkedudukan di luar negeri adalah pemimpin kantor cabang dan pejabat satu tingkat di bawah pemimpin kantor cabang.

12. Dewan Komisaris:

a) bagi Bank berbentuk badan hukum Perseroan Terbatas adalah dewan komisaris sebagaimana dimaksud dalam Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas;

b) bagi Bank berbentuk badan hukum:

1) Perusahaan Umum Daerah adalah dewan pengawas sebagaimana dimaksud dalam Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015;

2) Perusahaan Perseroan Daerah adalah komisaris sebagaimana dimaksud dalam Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015;

3) Perusahaan Daerah adalah pengawas pada Bank yang belum berubah bentuk menjadi Perusahaan Umum Daerah atau Perusahaan Perseroan Daerah sebagaimana dimaksud Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015;

c) bagi Bank berbentuk badan hukum Koperasi adalah pengawas sebagaimana dimaksud dalam Undang-Undang Nomor 25 Tahun 1992 tentang Perkoperasian;

d) bagi Bank yang berstatus sebagai kantor cabang dari bank yang berkedudukan di luar negeri adalah pihak yang ditunjuk untuk melaksanakan fungsi pengawasan.

BAB II
RUANG LINGKUP MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Pasal 2

(1) Bank wajib menerapkan manajemen risiko secara efektif dalam penggunaan Teknologi Informasi.

(2) Penerapan manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit mencakup:
   a. pengawasan aktif Direksi dan Dewan Komisaris;
   b. kecukupan kebijakan, standar, dan prosedur penggunaan Teknologi Informasi;
   c. kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko penggunaan Teknologi Informasi; dan
   d. sistem pengendalian intern atas penggunaan Teknologi Informasi.

(3) Penerapan manajemen risiko harus dilakukan secara terintegrasi dalam setiap tahapan penggunaan Teknologi Informasi sejak proses perencanaan,

pengadaan, pengembangan, operasional, pemeliharaan hingga penghentian dan penghapusan sumber daya Teknologi Informasi.

Pasal 3

Penerapan manajemen risiko dalam penggunaan Teknologi Informasi oleh Bank sebagaimana dimaksud dalam Pasal 2 wajib disesuaikan dengan tujuan, kebijakan usaha, ukuran dan kompleksitas usaha Bank.

BAB III

PENERAPAN MANAJEMEN RISIKO
TEKNOLOGI INFORMASI

Bagian Kesatu

Pengawasan Aktif Direksi dan Dewan Komisaris

Pasal 4

Bank wajib menetapkan wewenang dan tanggung jawab yang jelas dari Direksi, Dewan Komisaris, dan pejabat pada setiap jenjang jabatan yang terkait dengan penggunaan Teknologi Informasi.

Pasal 5

Wewenang dan tanggung jawab Direksi sebagaimana dimaksud dalam Pasal 4 paling sedikit mencakup:

a. menetapkan Rencana Strategis Teknologi Informasi dan kebijakan Bank terkait penggunaan Teknologi Informasi;
b. menetapkan kebijakan, standar, dan prosedur terkait penyelenggaraan Teknologi Informasi yang memadai dan mengomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna Teknologi Informasi;
c. memastikan:
    1. Teknologi Informasi yang digunakan Bank dapat mendukung perkembangan usaha Bank,

pencapaian tujuan bisnis Bank dan kelangsungan pelayanan terhadap nasabah Bank;

2. terdapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan Teknologi Informasi;
3. ketersediaan sistem pengelolaan pengamanan informasi (*information security management system*) yang efektif dan dikomunikasikan kepada satuan kerja pengguna dan penyelenggara Teknologi Informasi;
4. penerapan proses manajemen risiko dalam penggunaan Teknologi Informasi dilaksanakan secara memadai dan efektif;
5. kebijakan, standar, dan prosedur Teknologi Informasi diterapkan secara efektif pada satuan kerja pengguna dan penyelenggara Teknologi Informasi;
6. terdapat sistem pengukuran kinerja proses penyelenggaraan Teknologi Informasi yang paling sedikit dapat:
   a) mendukung proses pemantauan terhadap implementasi strategi;
   b) mendukung penyelesaian proyek pengembangan Teknologi Informasi;
   c) mengoptimalkan pendayagunaan sumber daya manusia dan investasi pada infrastruktur; dan
   d) meningkatkan kinerja proses penyelenggaraan Teknologi Informasi dan kualitas layanan penyampaian hasil proses kepada pengguna Teknologi Informasi.

Pasal 6

Wewenang dan tanggung jawab Dewan Komisaris sebagaimana dimaksud dalam Pasal 4 paling sedikit mencakup:

a. mengevaluasi, mengarahkan, dan memantau Rencana Strategis Teknologi Informasi dan kebijakan Bank terkait penggunaan Teknologi Informasi; dan
b. mengevaluasi pertanggungjawaban Direksi atas penerapan manajemen risiko dalam penggunaan Teknologi Informasi.

Pasal 7

(1) Bank wajib memiliki komite pengarah Teknologi Informasi (*Information Technology steering committe*).
(2) Komite pengarah Teknologi Informasi sebagaimana dimaksud pada ayat (1) bertanggung jawab memberikan rekomendasi kepada Direksi paling sedikit terkait dengan:
    a. Rencana Strategis Teknologi Informasi yang sejalan dengan rencana strategis kegiatan usaha Bank;
    b. perumusan kebijakan, standar, dan prosedur Teknologi Informasi yang utama;
    c. kesesuaian antara proyek Teknologi Informasi yang disetujui dengan Rencana Strategis Teknologi Informasi;
    d. kesesuaian antara pelaksanaan proyek Teknologi Informasi dengan rencana proyek yang disepakati (*project charter*);
    e. kesesuaian antara Teknologi Informasi dengan kebutuhan sistem informasi manajemen serta kebutuhan kegiatan usaha Bank;
    f. efektivitas langkah-langkah dalam meminimalkan risiko atas investasi Bank pada sektor Teknologi Informasi agar investasi Bank pada sektor Teknologi Informasi memberikan kontribusi terhadap pencapaian tujuan bisnis Bank;
    g. pemantauan atas kinerja Teknologi Informasi dan upaya peningkatan kinerja Teknologi Informasi;
    h. upaya penyelesaian berbagai masalah terkait Teknologi Informasi yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara

Teknologi Informasi secara efektif, efisien, dan tepat waktu; dan

i. kecukupan dan alokasi sumber daya yang dimiliki Bank.

(3) Komite pengarah Teknologi Informasi sebagaimana dimaksud pada ayat (1) paling sedikit beranggotakan:

a. direktur yang membawahkan satuan kerja Teknologi Informasi;

b. direktur yang membawahkan satuan kerja manajemen risiko;

c. pejabat tertinggi yang memimpin satuan kerja Teknologi Informasi; dan

d. pejabat tertinggi yang memimpin satuan kerja pengguna Teknologi Informasi.

(4) Komite pengarah Teknologi Informasi sebagaimana dimaksud pada ayat (3) diketuai oleh salah satu direktur Bank merangkap sebagai anggota.

Bagian Kedua
Kecukupan Kebijakan, Standar, dan Prosedur Penggunaan Teknologi Informasi di Bank

Pasal 8

(1) Bank wajib memiliki kebijakan, standar, dan prosedur penggunaan Teknologi Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dan wajib menerapkan kebijakan, standar, dan prosedur penggunaan Teknologi Informasi secara konsisten dan berkesinambungan.

(2) Kebijakan, standar, dan prosedur penggunaan Teknologi Informasi paling sedikit meliputi aspek:

a. manajemen;

b. pengembangan dan pengadaan;

c. operasional Teknologi Informasi;

d. jaringan komunikasi;

e. pengamanan informasi;

f. Rencana Pemulihan Bencana;

g. Layanan Perbankan Elektronik;

h. penggunaan pihak penyedia jasa Teknologi Informasi; dan

i. penyediaan jasa Teknologi Informasi oleh Bank.

(3) Bank wajib menetapkan limit risiko yang dapat ditoleransi untuk memastikan aspek terkait Teknologi Informasi sebagaimana dimaksud pada ayat (2) dapat berjalan dengan optimal.

(4) Bank wajib melakukan kaji ulang dan pengkinian kebijakan, standar dan prosedur sebagaimana dimaksud pada ayat (2) secara berkala.

(5) Bank wajib menetapkan jangka waktu kaji ulang dan pengkinian kebijakan, standar, dan prosedur sebagaimana dimaksud pada ayat (4) dalam kebijakan secara tertulis.

Pasal 9

(1) Bank wajib memiliki Rencana Strategis Teknologi Informasi yang mendukung rencana strategis kegiatan usaha Bank.

(2) Rencana Strategis Teknologi Informasi sebagaimana dimaksud pada ayat (1) wajib dicantumkan dalam rencana bisnis Bank.

Bagian Ketiga

Proses Manajemen Risiko Terkait Teknologi Informasi

Pasal 10

(1) Bank wajib memiliki kebijakan, standar, dan prosedur atas proses manajemen risiko Teknologi Informasi.

(2) Bank wajib melakukan proses manajemen risiko terkait penggunaan Teknologi Informasi.

(3) Proses manajemen risiko sebagaimana dimaksud pada ayat (2) dilakukan paling sedikit terhadap aspek terkait Teknologi Informasi sebagaimana dimaksud dalam Pasal 8 ayat (2).

(4) Dalam hal Bank menggunakan pihak penyedia jasa Teknologi Informasi, Bank wajib memastikan pihak

penyedia jasa Teknologi Informasi menerapkan manajemen risiko sebagaimana diatur dalam Peraturan Otoritas Jasa Keuangan ini.

Pasal 11

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

a. menetapkan dan menerapkan prosedur dan metodologi pengembangan dan pengadaan Teknologi Informasi secara konsisten;
b. menerapkan manajemen proyek dalam pengembangan sistem;
c. melakukan uji coba yang memadai pada saat pengembangan dan pengadaan suatu sistem, termasuk uji coba bersama satuan kerja pengguna, untuk memastikan keakuratan dan berfungsinya sistem sesuai kebutuhan pengguna serta kesesuaian sistem yang satu dengan sistem yang lain;
d. melakukan dokumentasi atas pengembangan dan pemeliharaan sistem;
e. memiliki manajemen perubahan sistem aplikasi;
f. memastikan sistem Teknologi Informasi Bank mampu menampilkan kembali informasi secara utuh; dan
g. mengukur urgensi pembuatan perjanjian tertulis (*escrow agreement*) atas perangkat lunak yang dianggap penting untuk kelangsungan operasional Bank dalam hal perangkat lunak dibuat oleh pihak lain dan kode sumber tidak diberikan kepada Bank.

Pasal 12

Bank wajib memastikan kelangsungan dan kestabilan operasional Teknologi Informasi serta memitigasi risiko yang berpotensi dapat mengganggu kegiatan operasional Bank.

Pasal 13

Bank wajib menyediakan jaringan komunikasi yang memenuhi prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

Pasal 14

Bagi bank umum konvensional yang memiliki unit usaha syariah wajib memiliki sistem yang dapat menghasilkan laporan terpisah bagi kegiatan unit usaha syariah.

Pasal 15

(1) Bank wajib memiliki Rencana Pemulihan Bencana.
(2) Bank wajib memastikan Rencana Pemulihan Bencana sebagaimana dimaksud pada ayat (1) dapat dilaksanakan secara efektif agar kelangsungan operasional Bank tetap berjalan saat terjadi bencana dan/atau gangguan pada sarana Teknologi Informasi yang digunakan Bank.
(3) Bank wajib melakukan uji coba atas Rencana Pemulihan Bencana terhadap seluruh aplikasi dan infrastruktur yang kritikal sesuai hasil analisis dampak bisnis (*business impact analysis*), paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan melibatkan pengguna Teknologi Informasi.
(4) Bank wajib melakukan kaji ulang Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 16

Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dengan memperhatikan paling sedikit:

a. pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) secara efektif dan efisien dengan memperhatikan kepatuhan terhadap ketentuan;

b. pengamanan informasi yang dilakukan terhadap aspek teknologi, sumber daya manusia, dan proses dalam penggunaan Teknologi Informasi;
c. pengamanan informasi yang diterapkan berdasarkan hasil penilaian terhadap risiko (*risk assessment*) pada informasi yang dimiliki Bank; dan
d. ketersediaan manajemen penanganan insiden dalam pengamanan informasi.

Bagian Keempat
Sistem Pengendalian dan Audit Intern atas
Penyelenggaraan Teknologi Informasi

Pasal 17

(1) Bank wajib melaksanakan sistem pengendalian intern secara efektif terhadap seluruh aspek penggunaan Teknologi Informasi.
(2) Sistem pengendalian intern sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:
    a. pengawasan oleh manajemen dan adanya budaya pengendalian;
    b. identifikasi dan penilaian risiko;
    c. kegiatan pengendalian dan pemisahan fungsi;
    d. sistem informasi, sistem akuntansi, dan sistem komunikasi; dan
    e. kegiatan pemantauan dan koreksi penyimpangan, yang dilakukan oleh satuan kerja operasional, satuan kerja audit intern maupun pihak lain.
(3) Sistem informasi, sistem akuntansi, dan sistem komunikasi sebagaimana dimaksud pada ayat (2) huruf d harus didukung oleh teknologi, sumber daya manusia, dan struktur organisasi Bank yang memadai.
(4) Kegiatan pemantauan dan tindakan koreksi penyimpangan sebagaimana dimaksud pada ayat (2) huruf e paling sedikit meliputi:

a. kegiatan pemantauan secara terus menerus;
b. pelaksanaan fungsi audit intern yang efektif dan menyeluruh; dan
c. perbaikan terhadap penyimpangan yang diidentifikasi oleh satuan kerja operasional, satuan kerja audit intern, dan/atau pihak lain.

Pasal 18

(1) Pelaksanaan fungsi audit intern Teknologi Informasi sebagaimana dimaksud dalam Pasal 17 ayat (4) huruf b memperhatikan kepatuhan terhadap ketentuan mengenai standar pelaksanaan fungsi audit intern.
(2) Dalam rangka memastikan pelaksanaan audit intern Teknologi Informasi sebagaimana dimaksud dalam Pasal 17 ayat (4) huruf b, Bank wajib memastikan ketersediaan jejak audit (*audit trail*) atas seluruh kegiatan penyelenggaraan Teknologi Informasi untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lain.
(3) Dalam hal terdapat keterbatasan kemampuan satuan kerja audit intern, pelaksanaan fungsi audit intern Teknologi Informasi sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh auditor ekstern.
(4) Bank wajib melaksanakan audit intern terhadap seluruh aspek dalam penyelenggaraan dan penggunaan Teknologi Informasi sesuai kebutuhan, prioritas, dan hasil analisis risiko Teknologi Informasi paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 19

(1) Bank wajib memiliki pedoman audit intern atas penggunaan Teknologi Informasi yang diselenggarakan oleh Bank sendiri dan/atau oleh pihak penyedia jasa Teknologi Informasi.

(2) Bank wajib melakukan kaji ulang atas fungsi audit intern atas penggunaan Teknologi Informasi paling sedikit 1 (satu) kali dalam 3 (tiga) tahun.

(3) Kaji ulang sebagaimana dimaksud pada ayat (2) wajib menggunakan jasa pihak ekstern yang independen.

(4) Bank wajib menyampaikan kepada Otoritas Jasa Keuangan:

a. hasil kaji ulang sebagaimana dimaksud pada ayat (3) disertai saran perbaikan sebagai bagian dari laporan kaji ulang; dan

b. hasil audit intern terhadap Teknologi Informasi sebagai bagian dari laporan pelaksanaan dan pokok-pokok hasil audit intern,

sebagaimana diatur dalam ketentuan mengenai penerapan standar pelaksanaan fungsi audit intern.

BAB IV
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK DAN/ATAU PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI

Bagian Kesatu
Umum

Pasal 20

(1) Bank menyelenggarakan Teknologi Informasi.

(2) Penyelenggaraan Teknologi Informasi sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh Bank sendiri dan/atau pihak penyedia jasa Teknologi Informasi.

(3) Dalam hal penyelenggaraan Teknologi Informasi Bank dilakukan oleh pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada ayat (2), Bank wajib:

a. bertanggung jawab atas penerapan manajemen risiko;

b. memiliki satuan kerja Teknologi Informasi;

c. memiliki pejabat tertinggi yang memimpin satuan kerja Teknologi Informasi;
d. mampu melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa;
e. memilih pihak penyedia jasa Teknologi Informasi berdasarkan analisa biaya dan manfaat (*cost and benefit analysis*) dengan mengikutsertakan satuan kerja Teknologi Informasi Bank;
f. memantau dan mengevaluasi keandalan pihak penyedia jasa Teknologi Informasi secara berkala yang menyangkut kinerja, reputasi penyedia jasa, dan kelangsungan penyediaan layanan;
g. memberikan akses kepada auditor intern, auditor ekstern, dan Otoritas Jasa Keuangan untuk memperoleh data dan informasi setiap kali dibutuhkan;
h. memberikan akses kepada Otoritas Jasa Keuangan terhadap Pangkalan Data secara tepat waktu, baik untuk data terkini maupun untuk data yang telah lalu; dan
i. memastikan pihak penyedia jasa Teknologi Informasi:
    1. memiliki tenaga ahli yang memiliki keandalan dengan didukung oleh sertifikat keahlian secara akademis dan/atau secara profesional sesuai dengan keperluan penyelenggaraan Teknologi Informasi;
    2. menerapkan prinsip pengendalian Teknologi Informasi (*Information Technology control*) secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen;
    3. menyediakan akses bagi auditor intern Bank, auditor ekstern yang ditunjuk oleh Bank, Otoritas Jasa Keuangan, dan/atau pihak lain yang sesuai dengan ketentuan peraturan

perundang-undangan berwenang untuk melakukan pemeriksaan dalam rangka memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan;

4. menyatakan tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang sesuai undang-undang berwenang untuk melakukan pemeriksaan, akan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan;
5. sebagai pihak terafiliasi, menjaga keamanan seluruh informasi termasuk rahasia Bank dan data pribadi nasabah;
6. hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) berdasarkan persetujuan Bank yang dibuktikan dengan dokumen tertulis;
7. melaporkan kepada Bank setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank;
8. menyampaikan hasil audit Teknologi Informasi yang dilakukan auditor independen secara berkala terhadap penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi, kepada Otoritas Jasa Keuangan melalui Bank yang bersangkutan;
9. menyediakan Rencana Pemulihan Bencana yang teruji dan memadai;
10. bersedia untuk kemungkinan penghentian perjanjian sebelum jangka waktu perjanjian berakhir (*early termination*); dan

11. memenuhi tingkat layanan sesuai dengan *service level agreement* antara Bank dan pihak penyedia jasa Teknologi Informasi.

(4) Penggunaan pihak penyedia jasa Teknologi Informasi oleh Bank sebagaimana dimaksud pada ayat (3) wajib didasarkan pada perjanjian tertulis yang paling sedikit memuat kesediaan pihak penyedia jasa Teknologi Informasi untuk menyelenggarakan dan/atau melakukan hal-hal sebagaimana dimaksud pada ayat (3) huruf i.

(5) Bank wajib melakukan proses seleksi dalam memilih pihak penyedia jasa Teknologi Informasi dengan memperhatikan prinsip kehati-hatian, manajemen risiko, dan didasarkan pada hubungan kerja sama secara wajar (*arm's length principle*), dalam hal pihak penyedia jasa Teknologi Informasi merupakan pihak terkait dengan Bank.

(6) Bank wajib melakukan tindakan tertentu dalam hal terdapat kondisi berupa:

a. memburuknya kinerja penyelenggaraan Teknologi Informasi oleh penyedia jasa Teknologi Informasi yang dapat berdampak signifikan pada kegiatan usaha Bank;

b. pihak penyedia jasa Teknologi Informasi menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan;

c. terdapat pelanggaran oleh pihak penyedia jasa Teknologi Informasi terhadap ketentuan rahasia Bank dan kewajiban merahasiakan data pribadi nasabah; dan/atau

d. terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan dalam rangka pengawasan oleh Otoritas Jasa Keuangan.

(7) Tindakan tertentu sebagaimana dimaksud pada ayat (6), paling sedikit:

a. melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi

sebagaimana dimaksud pada ayat (6) diketahui oleh Bank;

b. memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan jasa dalam hal diperlukan; dan

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

(8) Dalam hal penggunaan penyedia jasa Teknologi Informasi atau rencana penggunaan penyedia jasa Teknologi Informasi menyebabkan atau diindikasikan akan menyebabkan kesulitan pengawasan yang dilakukan oleh Otoritas Jasa Keuangan, Otoritas Jasa Keuangan dapat:

a. memerintahkan Bank untuk menghentikan penggunaan jasa Teknologi Informasi sebelum berakhirnya jangka waktu perjanjian; atau

b. menolak rencana penggunaan pihak penyedia jasa Teknologi Informasi yang diajukan oleh Bank.

Bagian Kedua
Penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana

Pasal 21

(1) Bank wajib menempatkan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia.

(2) Bank hanya dapat menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sepanjang mendapatkan persetujuan dari Otoritas Jasa Keuangan.

(3) Sistem Elektronik yang dapat ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar

wilayah Indonesia sebagaimana dimaksud pada ayat (2), adalah:

a. Sistem Elektronik yang digunakan untuk mendukung analisis terintegrasi dalam rangka memenuhi *home regulatory* yang bersifat global, termasuk lintas negara, sepanjang tidak terkait langsung dengan data individu nasabah dan data transaksi masing-masing nasabah, kecuali diatur lain oleh *home regulatory*.
b. Sistem Elektronik yang digunakan untuk manajemen risiko secara terintegrasi dengan kantor pusat atau kantor induk/kantor entitas utama di luar wilayah Indonesia, sepanjang menggunakan:
    1. data agregat nasabah; dan/atau
    2. data individu nasabah yang merupakan satu grup dengan nasabah di bank atau grup bank yang sama di luar wilayah Indonesia;
c. Sistem Elektronik yang digunakan dalam rangka penerapan anti pencucian uang dan pencegahan pendanaan terorisme secara terintegrasi dengan kantor pusat bank atau kantor induk bank di luar wilayah Indonesia, yang tidak terkait dengan data transaksi nasabah;
d. Sistem Elektronik yang digunakan untuk manajemen komunikasi antara kantor pusat dengan kantor cabang atau antara anak perusahaan dengan perusahaan induk; dan/atau
e. Sistem Elektronik yang digunakan untuk manajemen intern.

(4) Persetujuan Otoritas Jasa Keuangan sebagaimana dimaksud pada ayat (2) dapat diberikan dalam hal Bank:

a. memenuhi persyaratan sebagaimana dimaksud dalam Pasal 20 ayat (3), ayat (4), dan ayat (5);
b. menyampaikan hasil analisis *country risk*;

c. memastikan penyelenggaraan Sistem Elektronik di luar wilayah Indonesia tidak mengurangi efektifitas pengawasan Otoritas Jasa Keuangan yang dibuktikan dengan surat pernyataan;
d. memastikan bahwa informasi mengenai rahasia Bank hanya diungkapkan sepanjang memenuhi peraturan perundang-undangan di Indonesia yang dibuktikan dengan perjanjian kerja sama antara Bank dan pihak penyedia jasa Teknologi Informasi;
e. memastikan bahwa perjanjian tertulis dengan penyedia jasa Teknologi Informasi juga memuat klausula pilihan hukum (*choice of law*);
f. menyampaikan surat pernyataan tidak keberatan dari otoritas pengawas penyedia jasa Teknologi Informasi di luar wilayah Indonesia bahwa Otoritas Jasa Keuangan dapat melakukan pemeriksaan terhadap pihak penyedia jasa Teknologi Informasi;
g. menyampaikan surat pernyataan bahwa Bank akan menyampaikan secara berkala hasil penilaian yang dilakukan kantor bank di luar wilayah Indonesia atas penerapan manajemen risiko pada pihak penyedia jasa Teknologi Informasi;
h. memastikan manfaat dari rencana penempatan Sistem Elektronik di luar wilayah Indonesia bagi Bank lebih besar daripada beban yang ditanggung oleh Bank; dan
i. menyampaikan rencana Bank untuk meningkatkan kemampuan sumber daya manusia Bank baik yang berkaitan dengan penyelenggaraan Teknologi Informasi maupun transaksi bisnis atau produk yang ditawarkan.

Pasal 22

(1) Pusat Data dan Pusat Pemulihan Bencana sebagaimana dimaksud dalam Pasal 21 wajib menjamin kelangsungan usaha Bank.
(2) Pengelolaan Pusat Data dan Pusat Pemulihan Bencana sebagaimana dimaksud pada ayat (1), diatur lebih lanjut dalam Surat Edaran Otoritas Jasa Keuangan.

Bagian Ketiga
Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Penyedia Jasa

Pasal 23

(1) Bank wajib menyelenggarakan Pemrosesan Transaksi Berbasis Teknologi Informasi di wilayah Indonesia.
(2) Pemrosesan Transaksi Berbasis Teknologi Informasi dapat dilakukan oleh pihak penyedia jasa di wilayah Indonesia.
(3) Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak penyedia jasa sebagaimana dimaksud pada ayat (2) dapat dilakukan sepanjang:
    a. memenuhi prinsip kehati-hatian;
    b. memenuhi persyaratan sebagaimana dimaksud dalam Pasal 20 ayat (3), ayat (4), dan ayat (5); dan
    c. memperhatikan aspek perlindungan kepada nasabah.
(4) Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak penyedia jasa Teknologi Informasi dapat dilakukan di luar wilayah Indonesia sepanjang:
    a. memenuhi persyaratan sebagaimana dimaksud pada ayat (3);
    b. dokumen pendukung administrasi keuangan atas transaksi yang dilakukan di kantor Bank di Indonesia wajib ditatausahakan di kantor Bank di Indonesia;

c. Rencana bisnis Bank menunjukkan adanya upaya untuk meningkatkan peran Bank bagi perkembangan perekonomian Indonesia; dan
d. mendapatkan persetujuan terlebih dahulu oleh Otoritas Jasa Keuangan.

Pasal 24

(1) Bank wajib memuat rencana penggunaan pihak penyedia jasa Teknologi Informasi dalam penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi dalam Rencana Strategis Teknologi Informasi dan rencana bisnis Bank.
(2) Bank wajib melaporkan rencana penggunaan pihak penyedia jasa Teknologi Informasi dalam penyelenggaraan Pusat Data, Pusat Pemulihan Bencana dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi di wilayah Indonesia kepada Otoritas Jasa Keuangan paling lambat 2 (dua) bulan sebelum penyelenggaraan kegiatan oleh pihak penyedia jasa efektif dioperasikan.
(3) Dalam hal terdapat rencana menyelenggarakan Sistem Elektronik di luar wilayah Indonesia, Bank wajib menyampaikan permohonan persetujuan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan sebelum penyelenggaraan kegiatan oleh pihak penyedia jasa Teknologi Informasi efektif dioperasikan.
(4) Realisasi rencana penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Berbasis Teknologi Informasi oleh pihak penyedia jasa Teknologi Informasi wajib dilaporkan paling lambat 1 (satu) bulan sejak kegiatan efektif dioperasikan.
(5) Persetujuan atau penolakan atas permohonan sebagaimana dimaksud pada ayat (3) diberikan oleh Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah dokumen permohonan diterima secara lengkap dan memadai.

(6) Tata cara penyampaian rencana dan realisasi rencana sebagaimana dimaksud pada ayat (2), ayat (3), dan ayat (4) dilaksanakan dengan menggunakan format laporan penggunaan Teknologi Informasi yang diatur lebih lanjut dalam Surat Edaran Otoritas Jasa Keuangan.

Bagian Keempat

Penyediaan Jasa Teknologi Informasi oleh Bank

Pasal 25

(1) Bank dapat memberikan penyediaan jasa Teknologi Informasi kepada lembaga jasa keuangan lain:
   a. yang diawasi oleh Otoritas Jasa Keuangan, dan/atau
   b. di luar wilayah Indonesia.

(2) Bank wajib mendapat persetujuan dari Otoritas Jasa Keuangan dalam penyediaan jasa Teknologi Informasi kepada lembaga jasa keuangan sebagaimana dimaksud pada ayat (1).

(3) Persetujuan Otoritas Jasa Keuangan sebagaimana dimaksud pada ayat (2) dapat diberikan sepanjang Bank:
   a. memenuhi persyaratan penyediaan jasa Teknologi Informasi tidak menjadi salah satu kegiatan pokok Bank;
   b. memenuhi prinsip kehati-hatian;
   c. memperhatikan analisa biaya dan manfaat (*cost and benefit analysis*);
   d. memenuhi ketentuan peraturan perundang-undangan; dan
   e. memenuhi prinsip hubungan kerja sama secara wajar (*arm's length principle*).

(4) Penyediaan jasa Teknologi Informasi sebagaimana dimaksud pada ayat (1) hanya terbatas pada penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana.

(5) Bank dapat memberikan penyediaan jasa Teknologi Informasi berupa aplikasi dengan persetujuan Otoritas Jasa Keuangan, sepanjang:
   a. tetap memenuhi persyaratan pada ayat (3) dan lembaga jasa keuangan pengguna jasa Teknologi Informasi merupakan Bank; dan
   b. penyediaan jasa Teknologi Informasi untuk mendukung program inklusi Keuangan; dan/atau
   c. pengguna jasa Teknologi Informasi berada dalam konglomerasi yang sama.

Pasal 26

Penyediaan jasa Teknologi Informasi dalam rangka pengembangan layanan produk dan/atau aktivitas Bank dikecualikan dari pengaturan sebagaimana dimaksud dalam Pasal 25.

BAB V

LAYANAN PERBANKAN ELEKTRONIK

Pasal 27

(1) Bank yang menyelenggarakan Layanan Perbankan Elektronik wajib memenuhi ketentuan Otoritas Jasa Keuangan dan/atau otoritas lain yang terkait.
(2) Bank yang menyelenggarakan produk lanjutan Layanan Perbankan Elektronik yang dikategorikan sebagai layanan perbankan digital (*digital banking*) wajib memenuhi ketentuan Otoritas Jasa Keuangan.
(3) Ketentuan lebih lanjut mengenai layanan perbankan digital (*digital banking*) diatur dalam ketentuan Otoritas Jasa Keuangan.

Pasal 28

(1) Bank wajib memuat rencana penerbitan produk Layanan Perbankan Elektronik dalam rencana bisnis Bank.

(2) Bank yang akan menerbitkan produk Layanan Perbankan Elektronik yang bersifat transaksional wajib mengajukan permohonan persetujuan produk Layanan Perbankan Elektronik dan memperoleh persetujuan dari Otoritas Jasa Keuangan.

(3) Permohonan persetujuan produk Layanan Perbankan Elektronik sebagaimana dimaksud pada ayat (2) wajib dilengkapi dengan hal-hal sebagai berikut:

a. bukti kesiapan untuk menyelenggarakan Layanan Perbankan Elektronik yang paling sedikit memuat:
   1. struktur organisasi yang mendukung termasuk pengawasan dari pihak manajemen;
   2. kebijakan, sistem, prosedur dan kewenangan dalam penerbitan produk Layanan Perbankan Elektronik;
   3. kesiapan infrastruktur Teknologi Informasi untuk mendukung produk Layanan Perbankan Elektronik;
   4. hasil analisa dan identifikasi risiko yang melekat pada produk Layanan Perbankan Elektronik;
   5. kesiapan penerapan manajemen risiko khususnya pengendalian pengamanan (*security control*) untuk memastikan terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authentication*), tidak dapat diingkari (*non repudiation*), dan ketersediaan (*availability*);
   6. hasil analisa aspek hukum;
   7. uraian sistem informasi akuntansi; dan
   8. program perlindungan dan edukasi nasabah.
b. Hasil analisa bisnis mengenai proyeksi produk baru 1 (satu) tahun yang akan datang; dan
c. dokumen pendukung lain dalam hal diperlukan.

(4) Penyampaian permohonan sebagaimana dimaksud pada ayat (2) harus dilengkapi dengan hasil pemeriksaan dari pihak independen untuk memberikan pendapat atas karakteristik produk dan kecukupan pengamanan sistem Teknologi Informasi terkait produk serta kepatuhan terhadap ketentuan dan/atau praktik yang berlaku secara internasional.

(5) Penyelenggaraan Teknologi Informasi untuk kegiatan Layanan Perbankan Elektronik yang dilakukan oleh pihak penyedia jasa Teknologi Informasi, tunduk pada ketentuan sebagaimana diatur dalam Bab IV mengenai penyelenggaraan Teknologi Informasi oleh Bank dan/atau pihak penyedia jasa Teknologi Informasi.

Pasal 29

Bank wajib menerapkan prinsip pengendalian pengamanan data nasabah dan transaksi Layanan Perbankan Elektronik pada setiap Sistem Elektronik yang digunakan oleh Bank.

BAB VI
PELAPORAN

Bagian Pertama
Laporan Teknologi Informasi

Pasal 30

(1) Bank wajib melaporkan kondisi terkini penggunaan Teknologi Informasi paling lambat 1 (satu) bulan sejak akhir tahun pelaporan.

(2) Bank wajib melaporkan rencana pengembangan Teknologi Informasi yang akan diimplementasikan 1 (satu) tahun ke depan paling lambat tanggal 31 Oktober tahun sebelumnya.

(3) Rencana pengembangan Teknologi Informasi sebagaimana dimaksud pada ayat (2) dapat diubah 1 (satu) kali.

(4) Perubahan rencana pengembangan Teknologi Informasi sebagaimana dimaksud pada ayat (3) disampaikan paling lambat tanggal 30 Juni tahun berjalan.

(5) Bank dapat mengajukan perubahan rencana pengembangan Teknologi Informasi selain dalam jangka waktu sebagaimana dimaksud pada ayat (4) sepanjang memenuhi pertimbangan tertentu dan mendapatkan persetujuan dari Otoritas Jasa Keuangan.

(6) Otoritas Jasa Keuangan berwenang meminta Bank untuk melakukan penyesuaian terhadap perubahan rencana pengembangan Teknologi Informasi sebagaimana dimaksud pada ayat (2).

(7) Bank wajib melaporkan hasil audit Teknologi Informasi paling lambat 2 (dua) bulan setelah audit selesai dilakukan.

Bagian Kedua
Laporan Insidentil

Pasal 31

(1) Bank wajib melaporkan kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraaan Teknologi Informasi yang dapat dan/atau telah mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank.

(2) Laporan sebagaimana dimaksud pada ayat (1) wajib disampaikan dengan segera kepada Otoritas Jasa Keuangan melalui surat elektronik (*electronic mail*) atau telepon yang diikuti dengan laporan tertulis paling lama 7 (tujuh) hari kerja setelah kejadian kritis dan/atau penyalahgunaan atau kejahatan diketahui.

(3) Laporan tertulis sebagaimana dimaksud pada ayat (2) merupakan bagian dari laporan kondisi yang berpotensi menimbulkan kerugian yang signifikan

terhadap kondisi keuangan Bank sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan tentang Penerapan Manajemen Risiko Bagi Bank Umum.

Bagian Ketiga
Permohonan Persetujuan dan Laporan Realisasi

Pasal 32

(1) Bank yang memiliki rencana kegiatan sebagai penyedia jasa Teknologi Informasi sebagaimana dimaksud dalam Pasal 25 dan/atau menerbitkan produk Layanan Perbankan Elektronik sebagaimana dimaksud dalam Pasal 28, harus mengajukan permohonan persetujuan kepada Otoritas Jasa Keuangan paling lambat 2 (dua) bulan sebelum implementasi.

(2) Bank wajib menyampaikan laporan realisasi kegiatan sebagai penyedia jasa Teknologi Informasi sebagaimana dimaksud dalam Pasal 25 dan/atau menerbitkan produk Layanan Perbankan Elektronik sebagaimana dimaksud dalam Pasal 28 kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah implementasi.

(3) Bank yang:
   a. menyelenggarakan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 21; dan/atau
   b. menyerahkan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi kepada pihak penyedia jasa di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 23,

   harus mengajukan permohonan persetujuan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan sebelum rencana implementasi.

(4) Bank yang:

a. menyelenggarakan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 21; dan/atau

b. menyerahkan penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi kepada pihak penyedia jasa di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 23,

wajib menyampaikan laporan realisasi kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) bulan setelah implementasi.

(5) Bank harus melakukan implementasi rencana kegiatan sebagaimana dimaksud pada ayat (1) dan/atau ayat (3) paling lama 6 (enam) bulan sejak persetujuan diberikan oleh Otoritas Jasa Keuangan.

(6) Dalam hal Bank tidak melakukan implementasi rencana kegiatan sebagaimana dimaksud pada ayat (1) dan/atau ayat (3) dalam jangka waktu 6 (enam) bulan sejak persetujuan diberikan oleh Otoritas Jasa Keuangan sebagaimana dimaksud pada ayat (5), persetujuan Otoritas Jasa Keuangan menjadi tidak berlaku.

(7) Dalam hal persetujuan Otoritas Jasa Keuangan sudah tidak berlaku sebagaimana dimaksud pada ayat (6), dan Bank tetap akan melakukan implementasi rencana kegiatan bank sebagaimana dimaksud pada ayat (1) dan/atau ayat (3), Bank harus menyampaikan kembali permohonan persetujuan kepada Otoritas Jasa Keuangan.

Bagian Keempat

Format dan Alamat Penyampaian Laporan

Pasal 33

Format dan petunjuk penyusunan laporan sebagaimana dimaksud dalam Pasal 30, Pasal 31, dan Pasal 32 diatur dalam Surat Edaran Otoritas Jasa Keuangan.

Pasal 34

Permohonan persetujuan penggunaan penyedia jasa Teknologi Informasi di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 21 dan Pasal 23, permohonan persetujuan penerbitan produk Layanan Perbankan Elektronik sebagaimana dimaksud dalam Pasal 28, serta penyampaian laporan sebagaimana dimaksud dalam Pasal 30, Pasal 31, dan Pasal 32 disampaikan kepada Otoritas Jasa Keuangan dengan alamat:

a. Departemen Pengawasan Bank terkait, Departemen Perbankan Syariah atau Kantor Regional Otoritas Jasa Keuangan di Jakarta, bagi Bank yang berkantor pusat atau kantor cabang dari bank yang berkedudukan di luar negeri yang berada di wilayah Provinsi Daerah Khusus Ibukota Jakarta; atau
b. Kantor Regional Otoritas Jasa Keuangan atau Kantor Otoritas Jasa Keuangan setempat, sesuai wilayah tempat kedudukan kantor pusat Bank.

BAB VII

LAIN-LAIN

Pasal 35

(1) Otoritas Jasa Keuangan dapat melakukan pemeriksaan atau meminta Bank untuk melakukan pemeriksaan terhadap seluruh aspek terkait penggunaan Teknologi Informasi.

(2) Bank wajib menyediakan akses kepada Otoritas Jasa Keuangan untuk dapat melakukan pemeriksaan pada seluruh aspek terkait penyelenggaraan Teknologi Informasi yang diselenggarakan sendiri dan/atau yang diselenggarakan oleh pihak lain.

BAB VIII

SANKSI

Pasal 36

(1) Bank yang tidak melaksanakan ketentuan sebagaimana ditetapkan dalam Pasal 2 ayat (1), Pasal 3, Pasal 4, Pasal 7 ayat (1), Pasal 8 ayat (1), Pasal 8 ayat (3), Pasal 8 ayat (4), Pasal 8 ayat (5), Pasal 9, Pasal 10 ayat (1), Pasal 10 ayat (2), Pasal 10 ayat (4), Pasal 11, Pasal 12, Pasal 13, Pasal 14, Pasal 15, Pasal 16, Pasal 17 ayat (1), Pasal 18 ayat (2), Pasal 18 ayat (4), Pasal 19, Pasal 20 ayat (3), Pasal 20 ayat (4), Pasal 20 ayat (5), Pasal 20 ayat (6), Pasal 21 ayat (1), Pasal 23 ayat (1), Pasal 23 ayat (4), Pasal 24 ayat (1), Pasal 24 ayat (2), Pasal 24 ayat (3), Pasal 24 ayat (4), Pasal 25 ayat (2), Pasal 27 ayat (1), Pasal 27 ayat (2), Pasal 28 ayat (1), Pasal 28 ayat (2), Pasal 28 ayat (3), Pasal 29, dan/atau Pasal 35 ayat (2), Peraturan Otoritas Jasa Keuangan ini, dapat dikenakan sanksi administratif berupa:
   a. teguran tertulis;
   b. penurunan tingkat kesehatan berupa penurunan peringkat faktor tata kelola dalam penilaian tingkat kesehatan Bank;
   c. larangan untuk menerbitkan produk atau melaksanakan aktivitas baru;
   d. pembekuan kegiatan usaha tertentu; dan/atau
   e. pencantuman anggota Direksi, Dewan Komisaris, dan pejabat eksekutif dalam daftar tidak lulus melalui mekanisme penilaian kemampuan dan kepatutan.

(2) Sanksi sebagaimana dimaksud pada ayat (1) huruf b, huruf c, huruf d atau huruf e dapat dikenakan baik dengan atau tanpa didahului pengenaan sanksi teguran tertulis sebagaimana dimaksud pada ayat (1) huruf a.

Pasal 37

(1) Bank yang tidak memenuhi ketentuan pelaporan sebagaimana dimaksud dalam Pasal 30 ayat (1), Pasal 30 ayat (2), Pasal 30 ayat (7), Pasal 31 ayat (1), Pasal 31 ayat (2), Pasal 32 ayat (2), dan/atau Pasal 32 ayat (4) Peraturan Otoritas Jasa Keuangan ini dikenakan sanksi administratif berupa:
   a. denda sebesar Rp1.000.000,00 (satu juta rupiah) per hari keterlambatan per laporan; atau
   b. denda sebesar Rp50.000.000,00 (lima puluh juta rupiah) per laporan, bagi Bank yang belum menyampaikan laporan setelah 1 (satu) bulan sejak batas akhir waktu penyampaian laporan.

(2) Pengenaan sanksi denda sebagaimana dimaksud pada ayat (1) tidak menghilangkan kewajiban penyampaian laporan.

Pasal 38

(1) Bank yang menyampaikan laporan sebagaimana dimaksud dalam Pasal 30 ayat (1), Pasal 30 ayat (2), Pasal 30 ayat (7), Pasal 31 ayat (1), Pasal 31 ayat (2), Pasal 32 ayat (2), dan/atau Pasal 32 ayat (4), namun tidak sesuai dengan kondisi Bank yang sebenarnya dikenakan sanksi administratif berupa denda sebesar Rp50.000.000,00 (lima puluh juta rupiah).

(2) Bank dikenakan sanksi sebagaimana dimaksud pada ayat (1) setelah:
   a. Bank diberikan 2 (dua) kali surat teguran oleh Otoritas Jasa Keuangan dengan tenggang waktu 7 (tujuh) hari kerja untuk setiap teguran; dan

b. Bank tidak memperbaiki laporan dalam jangka waktu 7 (tujuh) hari kerja setelah surat teguran terakhir.

BAB IX
KETENTUAN PERALIHAN

Pasal 39

Bank yang telah memiliki kebijakan, standar, dan prosedur dalam penggunaan Teknologi Informasi dan pedoman manajemen risiko penggunaan Teknologi Informasi harus menyesuaikan dengan ketentuan dalam Peraturan Otoritas Jasa Keuangan ini paling lambat 12 (dua belas) bulan sejak berlakunya Peraturan Otoritas Jasa Keuangan ini.

Pasal 40

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

Pasal 41

(1) Bank yang telah menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebelum berlakunya Peraturan Otoritas Jasa Keuangan ini, harus memindahkan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi yang menyelenggarakan Sistem Elektronik untuk pelayanan publik ke Indonesia paling lambat tanggal 15 Oktober 2017.

(2) Dalam rangka pemindahan lokasi Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi dari luar wilayah Indonesia ke Indonesia, Bank harus menyampaikan laporan rencana tindak (*action plan*) kepada

Otoritas Jasa Keuangan paling lambat tanggal 30 Desember 2016.

BAB X
KETENTUAN PENUTUP

Pasal 42

Ketentuan lebih lanjut mengenai Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum diatur dalam Surat Edaran Otoritas Jasa Keuangan.

Pasal 43

(1) Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku, Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 144, Tambahan Lembaran Negara Republik Indonesia Nomor 4785) dicabut dan dinyatakan tidak berlaku.

(2) Peraturan pelaksanaan dari peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 144, Tambahan Lembaran Negara Republik Indonesia Nomor 4785) dinyatakan tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Peraturan Otoritas Jasa Keuangan ini.

Pasal 44

Peraturan Otoritas Jasa Keuangan ini mulai berlaku pada tanggal diundangkan dan ditetapkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Otoritas Jasa Keuangan ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 1 Desember 2016

KETUA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN,

ttd

MULIAMAN D. HADAD

Diundangkan di Jakarta
pada tanggal 7 Desember 2016

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

YASONNA H. LAOLY

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2016 NOMOR 267

Salinan sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Yuliana

PENJELASAN

ATAS

PERATURAN OTORITAS JASA KEUANGAN

NOMOR 38 /POJK.03/2016

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM

PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

I. UMUM

Dalam rangka meningkatkan efisiensi kegiatan operasional dan mutu pelayanan Bank kepada nasabahnya, Bank dituntut untuk mengembangkan strategi bisnis Bank dengan lebih optimal dalam memanfaatkan kemajuan Teknologi Informasi untuk meningkatkan daya saing Bank.

Penerapan Teknologi Informasi membawa perubahan dalam kegiatan operasional dan pengelolaan data Bank sehingga dapat dilakukan secara lebih efisien dan efektif serta memberikan informasi secara lebih akurat dan cepat. Perkembangan produk perbankan berbasis teknologi diantaranya berupa Layanan Perbankan Elektronik (*Electronic Banking*) dan layanan perbankan digital (*digital banking*), lebih memudahkan nasabah untuk melakukan transaksi perbankan secara non tunai setiap saat melalui jaringan elektronik. Selain itu penggunaan jasa pihak ketiga dalam penyediaan sistem dan pelayanan Bank semakin meningkat pula.

Di samping berbagai manfaat dan keunggulan yang diperoleh dari penggunaan Teknologi Informasi dalam pelaksanaan kegiatan operasional Bank, terdapat pula risiko yang dapat merugikan Bank dan nasabah seperti risiko operasional, risiko hukum, dan risiko reputasi, selain risiko perbankan lainnya seperti risiko likuiditas dan risiko kredit.

Oleh karena itu, agar dapat melindungi kepentingan Bank dan juga nasabah, Bank dituntut untuk menerapkan manajemen risiko secara efektif sehingga Bank dapat melakukan pengendalian dari kemungkinan penambahan risiko yang terjadi.

Mengingat bahwa Teknologi Informasi merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing Bank sementara dalam penyelenggaraannya mengandung berbagai risiko maka Bank perlu menerapkan tata kelola teknologi informasi (*information technology governance*). Keberhasilan penerapan tata kelola teknologi informasi sangat tergantung pada komitmen seluruh unit kerja di Bank, baik penyelenggara maupun pengguna Teknologi Informasi. Penerapan tata kelola teknologi informasi dilakukan melalui penyelarasan Rencana Strategis Teknologi Informasi dengan strategi bisnis Bank, optimalisasi pengelolaan sumber daya, pemanfaatan Teknologi Informasi (*Information Technology value delivery*), pengukuran kinerja, dan penerapan manajemen risiko yang efektif.

Untuk dapat menerapkan manajemen risiko yang efektif, diperlukan keterlibatan dan pengawasan Direksi dan Dewan Komisaris, penyusunan dan penerapan kebijakan, standar, dan prosedur terkait Teknologi Informasi serta proses identifikasi, pengukuran, pemantauan dan pengendalian risiko yang berkesinambungan.

Selain itu, pada masa yang akan datang Bank dituntut pula untuk mengantisipasi kebutuhan infrastruktur Teknologi Informasi yang memadai dalam rangka menghadapi implementasi kerangka Basel (*Basel framework*).

Seiring dengan perkembangan yang ada baik dalam lingkup nasional maupun internasional, sampai dengan saat ini telah dikeluarkan beberapa ketentuan peraturan perundang-undangan yang terkait dengan Teknologi Informasi antara lain Undang-Undang mengenai Informasi dan Transaksi Elektronik dan peraturan pelaksanaannya berupa Peraturan Pemerintah mengenai Penyelenggaraan Sistem dan Transaksi Elektronik serta Peraturan Menteri terkait. Selain itu, standar acuan penilaian terkait Teknologi Informasi seperti Standar Nasional Indonesia (SNI), *International Organization for Standarization* (ISO), *Control Objective for Information and Related Technology* (COBIT), dan *International Electrotechnical*

Commission (IEC) juga mengalami pengkinian sehingga menjadi lebih komprehensif dalam mendukung perkembangan dan implementasi Teknologi Informasi.

Dengan ketentuan ini, Bank diharapkan mampu mengelola risiko yang dihadapi secara efektif dalam seluruh aktivitas operasional yang didukung dengan pemanfaatan Teknologi Informasi.

II. PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2

Ayat (1)

Cukup Jelas.

Ayat (2)

Cukup Jelas.

Ayat (3)

Sumber daya Teknologi Informasi mencakup antara lain perangkat keras, perangkat lunak, jaringan, sumber daya manusia, data, dan informasi.

Perangkat keras adalah 1 (satu) atau serangkaian alat yang terhubung dalam Sistem Elektronik.

Perangkat lunak adalah 1 (satu) atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian Sistem Elektronik.

Pasal 3

Kompleksitas usaha meliputi antara lain keragaman dalam jenis transaksi, produk, jasa, jaringan kantor dan/atau teknologi pendukung yang digunakan.

Pasal 4

Dalam menetapkan wewenang dan tanggung jawab, Bank perlu memperhatikan antara lain prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*), misalnya pihak yang melakukan *input* data berbeda dari pihak yang melakukan validasi data.

Pasal 5

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Angka 1

Cukup jelas.

Angka 2

Peningkatan kompetensi sumber daya manusia antara lain melalui program pendidikan dan pelatihan secara berkesinambungan mengenai penyelenggaraan dan penggunaan Teknologi Informasi.

Angka 3

Cukup jelas.

Angka 4

Cukup jelas.

Angka 5

Cukup jelas.

Angka 6

Cukup jelas.

Pasal 6

Cukup jelas.

Pasal 7

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Struktur komite pengarah Teknologi Informasi dapat disesuaikan dengan ukuran dan kompleksitas kegiatan Bank serta struktur kepemilikan atau *legal entity* Bank.

Ayat (4)

Cukup jelas.

Pasal 8

Ayat (1)

Cukup jelas.

Ayat (2)

Kedalaman kebijakan, standar, dan prosedur penggunaan Teknologi Informasi disesuaikan dengan tujuan kebijakan usaha, ukuran dan kompleksitas usaha Bank, dan memperhatikan profil risiko Bank.

Huruf a

Yang dimaksud dengan “manajemen” antara lain Direksi, Dewan Komisaris, dan komite pengarah Teknologi Informasi.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.

Huruf g

Cukup jelas.

Huruf h

Cukup jelas.

Huruf i

Cukup jelas.

Ayat (3)

Yang dimaksud dengan “limit risiko” adalah tingkat kesalahan yang masih dapat ditoleransi oleh sistem (*risk tolerance*) atau standar pengamanan yang ditetapkan atau disetujui untuk tidak dilampaui.

Standar pengamanan sebagaimana dimaksud di atas disesuaikan dengan *risk appetite* yang dimiliki Bank.

Ayat (4)

Kaji ulang dan pengkinian dilakukan agar kebijakan, standar, dan prosedur tetap sesuai dengan perkembangan operasional Bank dan Teknologi Informasi.

Ayat (5)

Cukup jelas.

Pasal 9

Cukup jelas.

Pasal 10

Ayat (1)

Yang dimaksud dengan “proses manajemen risiko” adalah mengidentifikasi, mengukur, memantau, dan mengendalikan risiko.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 11

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Informasi yang ditampilkan kembali terkait dengan sistem yang tidak lagi digunakan dalam operasional Bank, *proprietary system*, maupun sistem yang masih digunakan

dalam operasional Bank namun mengalami gangguan.

Yang dimaksud dengan “secara utuh” adalah informasi yang ditampilkan lengkap dan akurat.

Huruf g

Yang dimaksud dengan “kode sumber” adalah suatu rangkaian perintah, pernyataan, dan/atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dapat dibaca dan dipahami.

Kode sumber ditempatkan pada pihak independen berdasarkan kesepakatan antara Bank dan pihak pembuat kode sumber.

Pasal 12

Cukup jelas.

Pasal 13

Cukup jelas.

Pasal 14

Yang dimaksud dengan “memiliki sistem yang dapat menghasilkan laporan terpisah” adalah sistem yang dapat mengidentifikasikan *input,* proses, dan *output* dari transaksi berdasarkan prinsip syariah.

Pasal 15

Ayat (1)

Cukup jelas.

Ayat (2)

Rencana Pemulihan Bencana mencakup rencana pemulihan pada berbagai tingkat bencana dan gangguan seperti:

a. *minor disaster* yang berdampak kecil dan tidak memerlukan biaya besar serta dapat diselesaikan dalam jangka waktu pendek;
b. *major disaster* yang berdampak besar dan dapat menjadi lebih parah apabila tidak diatasi segera; dan/atau
c. *catastrophic* yang berdampak terjadi kerusakan yang bersifat permanen sehingga memerlukan relokasi atau penggantian dengan biaya yang besar.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 16

Cukup jelas.

Pasal 17

Ayat (1)

Dalam melaksanakan sistem pengendalian intern Teknologi Informasi, Bank mengacu pada prinsip umum sebagaimana diatur dalam ketentuan mengenai pedoman standar sistem pengendalian intern.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang dimaksud dengan memadai antara lain teknologi yang sesuai dengan kegiatan operasional Bank, sumber daya manusia yang kompeten dan struktur organisasi yang tidak memberikan peluang untuk melakukan dan/atau menyembunyikan kesalahan atau penyimpangan.

Ayat (4)

Cukup jelas.

Pasal 18

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Penggunaan auditor ekstern untuk melaksanakan fungsi audit intern atas Teknologi Informasi tidak mengurangi tanggung jawab pimpinan satuan kerja audit intern. Selain itu penggunaan auditor ekstern harus mempertimbangkan ukuran dan kompleksitas usaha Bank serta memperhatikan ketentuan peraturan perundang-undangan terkait auditor ekstern.

Dalam hal Bank menggunakan auditor ekstern untuk melaksanakan fungsi audit intern atas Teknologi Informasi, proses *Entreprise Data Management* tetap harus dijalankan oleh satuan kerja audit intern.

Ayat (4)

Cukup jelas.

Pasal 19

Cukup jelas.

Pasal 20

Ayat (1)

Penyelenggaraan Teknologi Informasi antara lain penempatan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana.

Ayat (2)

Yang dimaksud dengan “menggunakan pihak penyedia jasa Teknologi Informasi” adalah penggunaan jasa pihak lain dalam penyelenggaraan Teknologi Informasi Bank secara berkesinambungan dan/atau dalam periode tertentu.

Yang dimaksud dengan pihak lain bagi:

a. kantor cabang dari bank yang berkedudukan di luar negeri termasuk kantor pusat dan kantor bank lain di luar negeri maupun kelompok usaha Bank; atau
b. bank yang dimiliki pihak asing termasuk kantor induk dan kelompok usaha Bank.

Selain itu, meskipun Bank menyerahkan penyelenggaraan Teknologi Informasi kepada pihak penyedia jasa maka Bank tetap disebut sebagai penyelenggara Sistem Elektronik untuk setiap Sistem Elektronik yang digunakan Bank dalam menjalankan kegiatan usahanya.

Ayat (3)

Huruf a

Yang dimaksud tanggung jawab Bank dalam menerapkan manajemen risiko antara lain dengan memastikan bahwa penyedia jasa Teknologi Informasi menerapkan manajemen risiko secara memadai pada

kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi sesuai dengan yang dipersyaratkan dalam Peraturan Otoritas Jasa Keuangan ini.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Yang dimaksud dengan "secara berkala" adalah pemantauan dan evaluasi keandalan pihak penyedia jasa Teknologi Informasi sesuai dengan *risk appetite* Bank terhadap jasa yang diberikan oleh pihak penyedia jasa Teknologi Informasi.

Huruf g

Akses untuk memperoleh data dan informasi dimaksudkan agar pemeriksaan dapat dilaksanakan secara efektif.

Huruf h

Akses terhadap Pangkalan Data meliputi namun tidak terbatas pada penyediaan terminal, *user id* untuk melakukan *query*, dan mengunduh data.

Huruf i

Angka 1

Cukup jelas.

Angka 2

Syarat ini dimaksudkan untuk meyakini bahwa Pusat Data, Pusat Pemulihan Bencana, dan/atau jasa Teknologi Informasi yang digunakan oleh Bank memiliki pengendalian Teknologi Informasi yang memadai paling sedikit mencakup pengamanan fisik dan pengamanan *logic*.

Angka 3

Akses sebagaimana dimaksud pada angka ini dibutuhkan untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan dalam rangka audit Teknologi Informasi, audit dan/atau pemeriksaan lain.

Auditor Otoritas Jasa Keuangan termasuk auditor ekstern yang ditunjuk oleh Otoritas Jasa Keuangan.

Angka 4

Cukup jelas.

Angka 5

Informasi termasuk sistem dan perangkat yang digunakan untuk memproses, menyimpan, dan mengirimkan informasi, merupakan aset yang harus dijamin keamanannya oleh pihak penyedia jasa dengan cara dilindungi dari musuh dan ancaman bahaya yang dapat mengganggu prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

Angka 6

Cukup jelas.

Angka 7

Cukup jelas.

Angka 8

Yang dimaksud dengan “secara berkala” adalah pelaksanaan audit sesuai dengan *risk appetite* Bank terhadap jasa yang diberikan oleh pihak penyedia jasa Teknologi Informasi.

Cakupan audit yang dilakukan oleh auditor independen termasuk sistem aplikasi yang digunakan untuk memproses data Bank.

Angka 9

Cukup jelas.

Angka 10

Cukup jelas.

Angka 11

Pemenuhan tingkat layanan dilakukan antara lain dengan memastikan penyelenggaraan Teknologi Informasi dapat mendukung Bank beroperasi sebagaimana mestinya.

Ayat (4)

Cukup jelas.

Ayat (5)

Yang dimaksud dengan "hubungan kerja sama secara wajar (*arm's length principle*)" adalah kondisi dimana transaksi antar pihak bersifat independen sebagaimana pihak yang tidak terkait, antara lain memiliki kesetaraan dan didasarkan pada harga pasar yang wajar sehingga meminimalisasi terjadinya benturan kepentingan (*conflict of interest*).

Yang dimaksud dengan "pihak terkait dengan Bank" adalah pihak terkait sebagaimana diatur dalam ketentuan mengenai batas maksimum pemberian kredit bank umum.

Ayat (6)

Huruf a

Cukup jelas.

Huruf b

Yang dimaksud dengan "insolven" adalah tidak memiliki cukup dana untuk melunasi utang.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Ayat (7)

Cukup jelas.

Ayat (8)

Indikasi kesulitan pengawasan antara lain:

a. kesulitan otoritas pengawas dalam melakukan akses terhadap data dan informasi;
b. kesulitan dalam pelaksanaan pemeriksaan terhadap pihak penyedia jasa Teknologi Informasi; dan/atau

c. pihak penyedia jasa Teknologi Informasi digunakan sebagai media untuk melakukan rekayasa data Bank dan/atau rekayasa keuangan Bank.

Pasal 21

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Yang dimaksud dengan "*home regulatory*" adalah ketentuan yang diterbitkan oleh otoritas negara asal bank.

Dalam hal ini *home regulatory* untuk kantor cabang adalah sesuai dengan kedudukan kantor pusat bank di luar negeri, sedangkan untuk kantor subsidiari sesuai dengan kedudukan kantor induk/kantor entitas utama, berupa bank di luar negeri.

Yang dimaksud aturan lain dalam hal ini adalah ketentuan dalam rangka untuk kepentingan publik atau negara, penegakan hukum, atau penerapan prinsip kehati-hatian.

Huruf b

Yang dimaksud dengan "nasabah yang merupakan satu grup" adalah nasabah lain yang mempunyai hubungan pengendalian dengan nasabah, sesuai dengan ketentuan mengenai batas maksimum pemberian kredit atau batas maksimum penyaluran dana.

Yang dimaksud dengan "grup bank yang sama" adalah kantor induk atau kantor entitas utama, anak perusahaan, atau perusahaan terelasi, yang berupa bank.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Ayat (4)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Yang dimaksud dengan “tidak mengurangi efektifitas pengawasan Otoritas Jasa Keuangan” adalah tidak menimbulkan kesulitan pengawas dalam memperoleh data dan informasi yang diperlukan seperti adanya akses terhadap Pangkalan Data dan memiliki struktur Pangkalan Data dari setiap aplikasi yang digunakan.

Huruf d

Ketentuan perundang-undangan yang berlaku di Indonesia antara lain ketentuan Otoritas Jasa Keuangan mengenai persyaratan dan tata cara pemberian perintah atau izin tertulis membuka rahasia Bank.

Huruf e

Cukup jelas.

Huruf f

Surat pernyataan disampaikan apabila pihak penyedia jasa Teknologi Informasi memiliki otoritas pengawasan.

Huruf g

Yang dimaksud dengan “kantor bank di luar wilayah Indonesia” adalah:

1. bagi kantor cabang dari bank yang berkedudukan di luar negeri yaitu kantor pusat atau kantor lainnya; atau
2. bagi Bank yang dimiliki lembaga keuangan asing yaitu kantor induk bank.

Surat pernyataan disampaikan termasuk apabila bank memiliki kantor bank di wilayah yang sama dengan wilayah kedudukan penyedia jasa Teknologi Informasi.

Huruf h

Manfaat yang diharapkan antara lain peningkatan kualitas layanan kepada nasabah serta penerapan program anti pencucian uang dan pencegahan pendanaan terorisme.

Huruf i

Cukup jelas.

Pasal 22

Ayat (1)

Yang dimaksud dengan “menjamin kelangsungan usaha” adalah memastikan bahwa kelangsungan usaha tetap dapat berjalan sebagaimana mestinya ketika terjadi bencana atau gangguan, termasuk menjamin kesiapan Sistem Elektronik yang terdapat dalam Pusat Data dan Pusat Pemulihan Bencana.

Ayat (2)

Cukup jelas.

Pasal 23

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Yang dimaksud dengan prinsip kehati-hatian dalam ayat ini antara lain mengenai pengelolaan risiko atas produk dan aktivitas baru sebagaimana diatur dalam ketentuan mengenai manajemen risiko.

Yang dimaksud dengan produk dan aktivitas baru antara lain produk dan aktivitas yang menambah atau meningkatkan risiko pada Bank termasuk pengembangan pelayanan seperti pemasaran kredit.

Huruf b

Cukup jelas.

Huruf c

Hubungan Bank dengan nasabah didasarkan atas perjanjian yang jelas dan memperhatikan ketentuan mengenai transparansi informasi produk dan penggunaan data pribadi nasabah serta ketentuan mengenai penyelesaian pengaduan nasabah.

Bank tetap bertanggung jawab atas setiap transaksi yang pemrosesannya diserahkan kepada pihak penyedia jasa.

Ayat (4)

Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar negeri dalam ayat ini termasuk yang dilakukan pada kantor pusat atau kantor lain bagi kantor cabang bank asing atau kantor induk bagi bank yang dimiliki lembaga keuangan asing.

Huruf a

Cukup jelas.

Huruf b

Yang dimaksud dengan "dokumen pendukung administrasi keuangan" adalah data yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha suatu perusahaan dan digunakan sebagai pendukung penyusunan laporan keuangan. Contoh: akad kredit dan dokumen pencairan kredit, *deal slip*, dan *deal confirmation* transaksi *treasury* serta dokumen perintah transfer data melalui *Society for Worldwide Interbank Financial Telecommunication* (SWIFT).

Huruf c

Upaya untuk meningkatkan peran Bank bagi perkembangan perekonomian Indonesia antara lain tercermin pada rencana peningkatan pemberian kredit dan peningkatan pembiayaan ekspor impor.

Huruf d

Cukup jelas.

Pasal 24

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Laporan tersebut mencakup kajian pascaimplementasi (*postimplemention review*).

Ayat (5)

Yang dimaksud dengan "dokumen permohonan diterima secara lengkap" adalah diterimanya dokumen yang dipersyaratkan dalam Peraturan Otoritas Jasa Keuangan ini serta diterimanya data tambahan dalam hal diperlukan.

Ayat (6)

Cukup jelas.

Pasal 25

Ayat (1)

Penyediaan jasa Teknologi Informasi oleh Bank adalah pemberian jasa berupa pemanfaatan infrastruktur Teknologi Informasi milik Bank kepada Lembaga Jasa Keuangan didasari dengan perjanjian kerjasama dan/atau sewa-menyewa di antara kedua belah pihak.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Pusat Data dan/atau Pusat Pemulihan Bencana termasuk jaringan komunikasi yang digunakan bersama oleh penyedia dan pengguna jasa Teknologi Informasi, namun tidak termasuk penyediaan aplikasi khusus bagi pengguna jasa.

Ayat (5)

Cukup jelas.

Pasal 26

Cukup jelas.

Pasal 27

Ayat (1)

Contoh Layanan Perbankan Elektronik antara lain *Automated Teller Machine* (ATM), *Cash Deposit Machine* (CDM), *phone banking*, *Short Message Services* (SMS) *banking*, *Electronic Data Capture* (EDC), *Point Of Sales* (POS), *internet banking*, dan *mobile banking*.

Ketentuan Otoritas Jasa Keuangan antara lain Peraturan Otoritas Jasa Keuangan mengenai Kegiatan Usaha dan Jaringan Kantor Bank Berdasarkan Modal Inti, ketentuan Otoritas Jasa Keuangan mengenai penerapan program anti pencucian uang dan pencegahan pendanaan terorisme bagi Bank, dan ketentuan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko serta ketentuan Otoritas Jasa Keuangan mengenai prinsip kehati-hatian dalam kegiatan usaha Bank.

Ketentuan otoritas lain yang terkait antara lain ketentuan mengenai penyelenggaraan kegiatan alat pembayaran menggunakan kartu.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 28

Ayat (1)

Cukup jelas.

Ayat (2)

Yang dimaksud dengan “produk Layanan Perbankan Elektronik” adalah produk baru yang memiliki karakteristik berbeda dengan produk yang telah ada di Bank dan/atau menambah atau meningkatkan eksposur risiko tertentu pada Bank.

Ayat (3)

Huruf a

Angka 1

Yang dimaksud dengan “manajemen” antara lain Direksi, Dewan Komisaris, dan Komite Pengarah Teknologi Informasi.

Angka 2

Cukup jelas.

Angka 3

Cukup jelas.

Angka 4

Cukup jelas.

Angka 5

Cukup jelas.

Angka 6

Cukup jelas.

Angka 7

Cukup jelas.

Angka 8

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Contoh dokumen pendukung lain antara lain dokumen yang dipersyaratkan oleh otoritas lain yang terkait, seperti:

1. tanda terdaftar Sistem Elektronik; dan
2. bukti perolehan sertifikasi Sistem Elektronik,

yang telah diterbitkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia, dan sesuai dengan ketentuan peraturan perundang-undangan yang mengatur mengenai penyelenggaraan sistem dan transaksi elektronik.

Ayat (4)

Hasil pemeriksaan dari pihak independen di luar Bank diperlukan untuk produk Layanan Perbankan Elektronik yang baru pertama kali diterbitkan oleh Bank seperti *internet*

banking yang bersifat transaksional dan SMS *banking*.

Untuk penambahan fitur layanan produk Layanan Perbankan Elektronik yang telah ada dan dapat menambah atau meningkatkan eksposur risiko, Bank dapat menyampaikan hasil pemeriksaan yang dilakukan oleh pihak intern Bank yang tidak ikut serta dalam perancangan dan pengembangan sistem aplikasi serta pengambilan keputusan dalam implementasi aktivitas Layanan Perbankan Elektronik.

Ayat (5)

Cukup jelas.

Pasal 29

Prinsip pengendalian pengamanan data nasabah dan transaksi Layanan Perbankan Elektronik pada setiap Sistem Elektronik mencakup:

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

Pasal 30

Ayat (1)

Laporan ini berisi perubahan yang telah dilakukan selama 1 (satu) tahun pelaporan atas data yang telah disampaikan dalam laporan penggunaan Teknologi Informasi, selain perubahan yang dilaporkan dalam tambahan rencana pengembangan Teknologi Informasi. Hal-hal yang perlu dilaporkan antara lain perubahan pejabat penentu dalam struktur organisasi Teknologi Informasi dan perubahan Rencana Strategis Teknologi Informasi.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Pertimbangan tertentu antara lain adalah untuk mendukung implementasi kebijakan dan/atau regulasi di sektor jasa keuangan dalam rangka mendorong perkembangan perekonomian.

Ayat (6)

Cukup jelas.

Ayat (7)

Audit Teknologi Informasi yang dimaksud antara lain audit Teknologi Informasi terhadap Pusat Data, Pusat Pemulihan Bencana, aplikasi, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi.

Pasal 31

Ayat (1)

Cukup jelas.

Ayat (2)

Laporan melalui surat elektronik (*electronic mail*) dan/atau telepon kepada satuan kerja pengawasan dari Bank berdasarkan informasi awal yang tersedia.

Ayat (3)

Cukup jelas.

Pasal 32

Ayat (1)

Bank dapat mengimplementasikan rencana kegiatan lebih awal dari 2 (dua) bulan sepanjang Otoritas Jasa Keuangan telah memberikan persetujuan atas permohonan persetujuan rencana kegiatan yang diajukan oleh Bank.

Ayat (2)

Laporan realisasi kegiatan sebagai penyedia jasa Teknologi Informasi dan penerbitan produk Layanan Perbankan Elektronik mencakup kajian pascaimplementasi (*postimplementation review*).

Ayat (3)

Bank dapat mengimplementasikan rencana kegiatan lebih awal dari 3 (tiga) bulan sepanjang Otoritas Jasa Keuangan telah memberikan persetujuan atas permohonan persetujuan rencana kegiatan yang diajukan oleh Bank.

Ayat (4)

Laporan realisasi penyelenggaraan Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia mencakup kajian pascaimplementasi (*postimplementation review*).

Ayat (5)

Cukup jelas.

Ayat (6)

Cukup jelas.

Ayat (7)

Cukup jelas.

Pasal 33

Cukup jelas.

Pasal 34

Cukup jelas.

Pasal 35

Ayat (1)

Cukup jelas.

Ayat (2)

Penyediaan akses kepada Otoritas Jasa Keuangan dimaksudkan agar pengawasan oleh Otoritas Jasa Keuangan dapat dilaksanakan secara efektif antara lain memastikan integritas, validitas, ketersediaan, dan keaslian data setiap transaksi yang dilakukan oleh Bank.

Akses kepada Otoritas Jasa Keuangan termasuk:

a. akses terhadap Pangkalan Data baik untuk data terkini maupun untuk data yang telah lalu; dan
b. akses terhadap infrastruktur pendukung seperti jaringan komunikasi.

Pasal 36

Cukup jelas.

Pasal 37

Cukup jelas.

Pasal 38

Cukup jelas.

Pasal 39

Cukup jelas.

Pasal 40

Cukup jelas.

Pasal 41

Ayat (1)

Cukup jelas.

Ayat (2)

Rencana tindak (*action plan*) antara lain berisi rencana pengembalian Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi ke dalam wilayah Indonesia dan jangka waktu penyelesaian rencana tindak (*action plan*).

Pasal 42

Cukup jelas.

Pasal 43

Cukup jelas.

Pasal 44

Cukup jelas.

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 5963