PERATURAN BANK INDONESIA

NOMOR: 9/15/PBI/2007

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR BANK INDONESIA,

Menimbang:

a. bahwa perkembangan Teknologi Informasi memungkinkan Bank memanfaatkannya 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 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 menggunakannya;

e. bahwa …

e. bahwa dalam rangka implementasi *Basel II* diperlukan infrastruktur Teknologi Informasi yang memadai;

f. bahwa sehubungan dengan pertimbangan sebagaimana dimaksud pada huruf a, huruf b, huruf c, huruf d dan huruf e, perlu ditetapkan ketentuan yang mengatur Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum dalam Peraturan Bank Indonesia;

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 23 Tahun 1999 tentang Bank Indonesia sebagaimana telah diubah dengan Undang-Undang Nomor 3 tahun 2004 (Lembaran Negara Tahun 1999 Nomor 66; Tambahan Lembaran Negara Nomor 3843);

3. Peraturan Bank Indonesia Nomor 5/8/PBI/2003 tentang Penerapan Manajemen Risiko bagi Bank Umum (Lembaran Negara Tahun 2003 Nomor 56; Tambahan Lembaran Negara Nomor 4292);

MEMUTUSKAN: …

MEMUTUSKAN:

Menetapkan: PERATURAN BANK INDONESIA TENTANG PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bank Indonesia 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 bank asing.
2. Teknologi Informasi adalah teknologi terkait sarana komputer, telekomunikasi dan sarana elektronis lainnya yang digunakan dalam pengolahan data keuangan dan atau pelayanan jasa perbankan.
3. Layanan Perbankan Melalui Media Elektronik atau selanjutnya disebut *Electronic Banking* adalah layanan yang memungkinkan nasabah Bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik antara lain ATM, *phone banking*, *electronic fund transfer, internet banking, mobile phone.*
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 tersebut dan prinsip-prinsip utama yang menjadi acuan dalam penggunaan Teknologi

Informasi untuk memenuhi kebutuhan bisnis dan mendukung rencana strategis jangka panjang.

5. Pusat Data (*Data Center)* adalah fasilitas utama pemrosesan data Bank yang terdiri dari perangkat keras dan perangkat lunak untuk mendukung kegiatan operasional Bank secara berkesinambungan.
6. *Database* adalah sekumpulan data komprehensif dan disusun secara sistematis, dapat diakses oleh pengguna sesuai wewenang masing-masing, dan dikelola oleh *database administrator*.
7. *Disaster Recovery Center* (DRC) adalah fasilitas pengganti pada saat Pusat Data (*Data Center*) mengalami gangguan atau tidak dapat berfungsi antara lain karena tidak adanya aliran listrik ke ruang komputer, kebakaran, ledakan atau kerusakan pada komputer, yang digunakan sementara waktu selama dilakukannya pemulihan Pusat Data Bank untuk menjaga kelangsungan kegiatan usaha (*business continuity*).
8. *Business Continuity Plan* (BCP) adalah kebijakan dan prosedur yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan/bencana dan proses pemulihan agar kegiatan operasional Bank dan pelayanan kepada nasabah tetap dapat berjalan.
9. Pemrosesan Transaksi Berbasis Teknologi adalah kegiatan berupa penambahan, perubahan, penghapusan, dan/atau otorisasi data yang dilakukan pada sistem aplikasi yang digunakan untuk memproses transaksi.
10. Komisaris :
    a. bagi Bank berbentuk hukum perseroan terbatas adalah dewan komisaris sebagaimana dimaksud dalam Pasal 1 angka 6 Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas;

b. bagi Bank berbentuk hukum perusahaan daerah adalah pengawas sebagaimana dimaksud dalam Pasal 19 Undang-Undang Nomor 5 Tahun 1962 tentang Perusahaan Daerah;

c. bagi Bank berbentuk hukum koperasi adalah pengawas sebagaimana dimaksud dalam Pasal 38 Undang-Undang Nomor 25 Tahun 1992 tentang Perkoperasian;

d. bagi kantor cabang bank asing adalah pejabat yang ditunjuk kantor pusat bank asing untuk melakukan fungsi pengawasan.

11. Direksi:

a. bagi Bank berbentuk hukum perseroan terbatas adalah direksi sebagaimana dimaksud dalam Pasal 1 angka 5 Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas;

b. bagi Bank berbentuk hukum perusahaan daerah adalah direksi sebagaimana dimaksud dalam Pasal 11 Undang Nomor 5 Tahun 1962 tentang Perusahaan Daerah;

c. bagi Bank berbentuk hukum koperasi adalah pengurus sebagaimana dimaksud dalam Pasal 29 Undang-Undang Nomor 25 Tahun 1992 tentang Perkoperasian;

d. bagi kantor cabang bank asing adalah pimpinan kantor cabang bank asing.

BAB II
RUANG LINGKUP MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Pasal 2

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

(2) Penerapan …

(2) Penerapan manajemen risiko sebagaimana dimaksud pada ayat (1) paling kurang mencakup:
   a. pengawasan aktif dewan Komisaris dan Direksi;
   b. kecukupan kebijakan 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 DALAM PENGGUNAAN TEKNOLOGI INFORMASI

Bagian Pertama
Pengawasan Aktif Dewan Komisaris dan Direksi

Pasal 4

Bank wajib menetapkan wewenang dan tanggung jawab yang jelas pada setiap jenjang jabatan yang terkait dengan penggunaan Teknologi Informasi.

Pasal 5 …

Pasal 5

Wewenang dan tanggung jawab sebagaimana dimaksud dalam Pasal 4 bagi dewan Komisaris paling kurang mencakup:

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

Pasal 6

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

a. menetapkan Rencana Strategis Teknologi Informasi dan kebijakan Bank terkait penggunaan Teknologi Informasi;
b. memastikan bahwa :
    1. Teknologi Informasi yang digunakan Bank dapat mendukung perkembangan usaha, pencapaian tujuan bisnis Bank dan kelangsungan pelayanan kepada nasabah;
    2. terdapat upaya peningkatan kompetensi sumber daya manusia yang terkait dengan penggunaan Teknologi Informasi;
    3. penerapan proses manajemen risiko dalam penggunaan Teknologi Informasi dilaksanakan secara memadai dan efektif;
    4. tersedianya kebijakan dan prosedur Teknologi Informasi yang memadai dan dikomunikasikan serta diterapkan secara efektif baik pada satuan kerja penyelenggara maupun pengguna Teknologi Informasi;

5. terdapat sistem pengukuran kinerja proses penyelenggaraan Teknologi Informasi yang paling kurang dapat:
   a) mendukung proses pemantauan terhadap implementasi strategi;
   b) mendukung penyelesaian proyek;
   c) mengoptimalkan pendayagunaan sumber daya manusia dan investasi pada infrastruktur;
   d) meningkatkan kinerja proses penyelenggaraan Teknologi Informasi dan kualitas layanan penyampaian hasil proses kepada pengguna.

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 yang paling kurang terkait dengan:
   a. Rencana Strategis Teknologi Informasi (*Information Technology Strategic Plan)* yang searah dengan rencana strategis kegiatan usaha Bank;
   b. kesesuaian proyek-proyek Teknologi Informasi yang disetujui dengan Rencana Strategis Teknologi Informasi;
   c. kesesuaian antara pelaksanaan proyek-proyek Teknologi Informasi dengan rencana proyek yang disepakati (*project charter*);
   d. kesesuaian Teknologi Informasi dengan kebutuhan sistem informasi manajemen dan kebutuhan kegiatan usaha Bank;

e. efektivitas langkah-langkah meminimalkan risiko atas investasi Bank pada sektor Teknologi Informasi agar investasi tersebut memberikan kontribusi terhadap tercapainya tujuan bisnis Bank;

f. pemantauan atas kinerja Teknologi Informasi dan upaya peningkatannya;

g. upaya penyelesaian berbagai masalah terkait Teknologi Informasi, yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara, secara efektif, efisien dan tepat waktu.

(3) Komite Pengarah Teknologi Informasi sebagaimana dimaksud pada ayat (1) paling kurang beranggotakan:

a. direktur yang membawahi satuan kerja Teknologi Informasi;

b. direktur yang membawahi satuan kerja Manajemen Risiko;

c. pejabat tertinggi yang membawahi satuan kerja penyelenggara Teknologi Informasi;

d. pejabat tertinggi yang membawahi satuan kerja pengguna utama Teknologi Informasi.

Bagian Kedua

Kecukupan Kebijakan dan Prosedur Penggunaan

Teknologi Informasi di Bank

Pasal 8

(1) Bank wajib memiliki kebijakan dan prosedur penggunaan Teknologi Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b.

(2) Kebijakan dan prosedur penggunaan Teknologi Informasi paling kurang meliputi aspek-aspek sebagai berikut :

a. Manajemen;
b. Pengembangan dan pengadaan;
c. Operasional Teknologi Informasi;
d. Jaringan komunikasi;
e. Pengamanan informasi*;*
f. *Business Continuity Plan;*
g. *End user computing*;
h. *Electronic Banking*; dan
i. Penggunaan pihak penyedia jasa Teknologi Informasi.

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

Pasal 9

(1) Bank wajib memiliki Rencana Strategis Teknologi Informasi (*Information Technology Strategic Plan*) yang mendukung rencana strategis kegiatan usaha Bank.
(2) Rencana Strategis Teknologi Informasi sebagaimana dimaksud pada ayat (1) dijabarkan dalam Rencana Bisnis Bank.

Bagian Ketiga

Proses Manajemen Risiko Terkait Teknologi Informasi

Pasal 10

(1) Bank wajib melakukan proses manajemen risiko yang mencakup identifikasi, pengukuran, pemantauan dan pengendalian atas risiko terkait penggunaan Teknologi Informasi.

(2) Proses manajemen risiko dilakukan terhadap aspek-aspek terkait Teknologi Informasi yang paling kurang mencakup pengembangan dan pengadaan Teknologi Informasi, operasional Teknologi Informasi, jaringan komunikasi, pengamanan informasi, *Business Continuity Plan, end user computing*, *Electronic Banking,* dan penggunaan pihak penyedia jasa Teknologi Informasi.

(3) Dalam hal Bank menggunakan jasa pihak lain untuk menyelenggarakan Teknologi Informasi, Bank wajib memastikan bahwa pihak penyedia jasa Teknologi Informasi menerapkan juga manajemen risiko yang paling kurang sesuai dengan ketentuan dalam Peraturan Bank Indonesia ini.

Pasal 11

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

a. menetapkan dan menerapkan prosedur dan metodologi pengembangan dan pengadaan Teknologi Informasi secara konsisten;
b. menerapkan manajemen proyek dalam pengembangan sistem;
c. melakukan *testing* 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 satu sistem dengan sistem yang lain;
d. melakukan dokumentasi sistem yang dikembangkan dan pemeliharaannya;
e. memiliki manajemen perubahan sistem aplikasi.

Pasal 12 …

Pasal 12

(1) Bank wajib mengidentifikasi dan memantau serta mengendalikan risiko yang terdapat pada aktivitas operasional Teknologi Informasi, pada jaringan komunikasi serta pada *end user computing* untuk memastikan efektifitas, efisiensi dan keamanan aktivitas tersebut antara lain dengan :
   a. menerapkan pengendalian fisik dan lingkungan terhadap fasilitas Pusat Data (*Data Center)* dan *Disaster Recovery Center*;
   b. menerapkan pengendalian hak akses secara memadai sesuai kewenangan yang ditetapkan;
   c. menerapkan pengendalian pada saat input, proses, dan output dari informasi;
   d. memperhatikan risiko yang mungkin timbul dari ketergantungan Bank terhadap penggunaan jaringan komunikasi;
   e. memastikan aspek desain dan pengoperasian dalam implementasi jaringan komunikasi sesuai dengan kebutuhan;
   f. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk adanya *audit trail*;
   g. melakukan pemantauan penggunaan aplikasi yang dikembangkan atau diadakan oleh satuan kerja di luar satuan kerja Teknologi Informasi.

(2) Bagi Bank yang memiliki unit usaha yang melaksanakan kegiatan usaha berdasarkan prinsip syariah, wajib memiliki sistem yang dapat menghasilkan laporan yang terpisah bagi kegiatan usaha Bank berdasarkan prinsip syariah.

Pasal 13 …

Pasal 13

(1) Bank wajib memastikan *Business Continuity Plan* dan *Disaster Recovery Plan* dapat dilaksanakan secara efektif agar kegiatan usaha Bank tetap berjalan saat terjadi gangguan yang signifikan pada sarana Teknologi Informasi yang digunakan Bank.

(2) Bank wajib melakukan uji coba atas *Business Continuity Plan* dan *Disaster Recovery Plan* terhadap seluruh sistem/aplikasi dan infrastruktur yang kritikal sesuai hasil *Business Impact Analysis*, paling kurang sekali dalam 1 (satu) tahun dengan melibatkan *end user (end to end)*.

(3) Bank wajib melakukan pengkinian *Business Continuity Plan* dan *Disaster Recovery Plan*.

Pasal 14

Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dengan memperhatikan paling kurang hal-hal sebagai berikut:

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

b. pengamanan informasi dilakukan terhadap aspek teknologi, sumber daya manusia dan proses dalam penggunaan Teknologi Informasi;

c. pengamanan informasi mencakup pengelolaan aset bank yang terkait dengan informasi, kebijakan sumber daya manusia, pengamanan fisik, pengamanan akses, pengamanan operasional, dan aspek penggunaan Teknologi Informasi lainnya;

d. adanya manajemen penanganan insiden dalam pengamanan informasi; dan

e. pengamanan informasi diterapkan berdasarkan hasil penilaian terhadap risiko (*risk assessment*) pada informasi yang dimiliki Bank.

Bagian Keempat

Sistem Pengendalian dan Audit Intern atas Penyelenggaraan Teknologi Informasi

Pasal 15

(1) Bank wajib melaksanakan sistem pengendalian intern secara efektif terhadap semua aspek penggunaan Teknologi Informasi.

(2) Sistem pengendalian intern sebagaimana dimaksud pada ayat (1) paling kurang mencakup:

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;

e. kegiatan pemantauan dan koreksi penyimpangan, yang dilakukan oleh satuan kerja operasional, satuan kerja audit intern maupun pihak lainnya.

(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 kurang meliputi:

a. kegiatan pemantauan secara terus menerus;

b. pelaksanaan fungsi audit intern yang efektif dan menyeluruh;

c. perbaikan terhadap penyimpangan baik yang diidentifikasi oleh satuan kerja operasional, satuan kerja audit intern maupun pihak lainnya.

Pasal 16

(1) Pelaksanaan fungsi audit intern Teknologi Informasi sebagaimana dimaksud dalam Pasal 15 ayat (4) huruf b memperhatikan kepatuhan terhadap ketentuan yang berlaku.
(2) Dalam hal terdapat keterbatasan kemampuan satuan kerja audit intern Teknologi Informasi maka pelaksanaan fungsi audit intern sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh auditor ekstern.
(3) Pelaksanaan audit intern wajib dilakukan secara berkala.

Pasal 17

(1) Pedoman audit intern yang dimiliki Bank wajib mencakup audit intern terhadap penggunaan Teknologi Informasi baik yang diselenggarakan sendiri atau oleh pihak penyedia jasa Teknologi Informasi.
(2) Bank wajib menyampaikan 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.
(3) Bank wajib melakukan kaji ulang atas fungsi audit intern atas penggunaan Teknologi Informasi paling kurang setiap 3 (tiga) tahun sekali.
(4) Kaji ulang sebagaimana dimaksud pada ayat (3) wajib menggunakan jasa pihak ekstern yang independen.

(5) Hasil kaji ulang disertai saran perbaikan dilaporkan kepada Bank Indonesia sebagai bagian dari laporan kaji ulang sebagaimana diatur dalam ketentuan mengenai penerapan standar pelaksanaan fungsi audit intern.

BAB IV
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI

Bagian Pertama
Umum
Pasal 18

(1) Bank dapat menyelenggarakan Teknologi Informasi sendiri dan/atau menggunakan pihak penyedia jasa Teknologi Informasi.

(2) Penggunaan pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada ayat (1) hanya dapat dilakukan sepanjang Bank dan pihak penyedia jasa Teknologi Informasi memenuhi persyaratan sebagai berikut:

a. bagi Bank:

1) Bank tetap bertanggung jawab atas penerapan manajemen risiko;

2) Bank mampu untuk melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi;

3) pemilihan pihak penyedia jasa Teknologi Informasi dilakukan oleh Bank berdasarkan *cost and benefit analysis* dan melibatkan satuan kerja penyelenggara Teknologi Informasi Bank;

4) Bank wajib memantau dan mengevaluasi kehandalan pihak penyedia jasa secara berkala baik yang menyangkut kinerja, reputasi penyedia jasa dan kelangsungan penyediaan layanan;

5) Bank …

5) Bank tetap memberikan akses kepada auditor intern, ekstern dan Bank Indonesia untuk memperoleh data dan informasi setiap kali dibutuhkan;

6) Bank memberikan akses kepada Bank Indonesia terhadap *database* secara tepat waktu baik untuk data terkini maupun untuk data yang telah lalu.

b. bagi pihak penyedia jasa Teknologi Informasi:

1) pihak penyedia jasa harus menerapkan prinsip pengendalian Teknologi Informasi (*IT control*) secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen;

2) pihak penyedia jasa harus menyediakan akses bagi auditor intern Bank, auditor ekstern yang ditunjuk oleh Bank, dan auditor Bank Indonesia untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan;

3) pihak penyedia jasa harus menyatakan tidak berkeberatan bila Bank Indonesia hendak melakukan pemeriksaan terhadap kegiatan penyediaan jasa tersebut;

4) sebagai pihak terafiliasi, pihak penyedia jasa harus menjamin keamanan seluruh informasi termasuk rahasia Bank dan data pribadi nasabah;

5) pihak penyedia jasa hanya dapat melakukan subkontrak sebagian kegiatannya berdasarkan persetujuan Bank yang dibuktikan dengan dokumen tertulis;

6) pihak penyedia jasa harus melaporkan kepada Bank setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank;

7) pihak …

7) pihak penyedia jasa harus menyampaikan secara berkala hasil audit Teknologi Informasi yang dilakukan auditor independen terhadap penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi, kepada Bank Indonesia melalui Bank yang bersangkutan;

8) pihak penyedia jasa harus menyediakan *Disaster Recovery Plan* yang teruji dan memadai; dan

9) pihak penyedia jasa harus bersedia untuk kemungkinan penghentian perjanjian sebelum berakhirnya jangka waktu perjanjian (*early termination*).

(3) Penggunaan pihak penyedia jasa Teknologi Informasi oleh Bank sebagaimana dimaksud pada ayat (1) harus didasarkan pada perjanjian tertulis yang paling kurang memuat kesediaan pihak penyedia jasa Teknologi Informasi untuk menyelenggarakan dan atau melakukan hal-hal sebagaimana dimaksud dalam ayat (2) huruf b.

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

(5) Dalam hal terdapat kondisi sebagai berikut:

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

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

c. terdapat …

c. terdapat pelanggaran oleh pihak penyedia jasa 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 Bank Indonesia;

maka Bank wajib melakukan hal-hal sebagai berikut:

a. melaporkan kepada Bank Indonesia paling lambat 3 (tiga) hari kerja setelah kondisi tersebut diatas diketahui oleh Bank;

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

c. melaporkan kepada Bank Indonesia segera setelah Bank menghentikan penggunaan jasa sebelum berakhirnya jangka waktu perjanjian.

(6) Dalam hal penggunaan penyedia jasa atau rencana penggunaan penyedia jasa menyebabkan atau diindikasikan akan menyebabkan kesulitan pengawasan yang dilakukan Bank Indonesia maka Bank Indonesia dapat:

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

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

Bagian Kedua

Penyelenggaraan Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center*

Pasal 19

(1) Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* diselenggarakan di dalam negeri.

(2) Dalam …

(2) Dalam hal Bank akan menyelenggarakan Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* di luar negeri, Bank harus mendapat persetujuan terlebih dahulu dari Bank Indonesia dengan memenuhi persyaratan tertentu.

(3) Persetujuan sebagaimana dimaksud pada ayat (2) dapat diberikan apabila Bank memenuhi persyaratan sebagaimana tercantum pada Pasal 18 ayat (2) sampai dengan ayat (4) serta persyaratan tambahan sebagai berikut:

a. Bank menyampaikan hasil analisis *country risk;*

b. Bank memastikan penyelenggaraan Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* di luar negeri tidak mengurangi efektifitas pengawasan Bank Indonesia;

c. Bank memastikan bahwa informasi mengenai rahasia Bank hanya dapat diungkapkan sepanjang memenuhi ketentuan perundang-undangan yang berlaku di Indonesia;

d. Bank memastikan bahwa perjanjian tertulis dengan penyedia jasa juga memuat klausula *choice of law*;

e. Apabila Bank merupakan kantor cabang bank asing atau Bank yang dimiliki lembaga keuangan asing maka Bank wajib menyampaikan:

1) Surat Pernyataan dari otoritas pengawas lembaga keuangan di luar negeri bahwa pihak penyedia jasa merupakan cakupan pengawasannya;

2) Surat Pernyataan tidak keberatan dari otoritas pengawas lembaga keuangan di luar negeri bahwa Bank Indonesia dapat melakukan pemeriksaan terhadap pihak penyedia jasa;

3) Surat Pernyataan bahwa Bank akan menyampaikan secara berkala hasil penilaian yang dilakukan kantor bank di luar negeri atas penerapan manajemen risiko pada pihak penyedia jasa.

f. Permohonan …

f. Permohonan persetujuan yang diajukan Bank harus memuat pula hal-hal sebagai berikut:
   1) Manfaat bagi Bank lebih besar daripada beban yang ditanggung oleh Bank;
   2) Rencana Bank untuk meningkatkan kemampuan sumber daya manusia Bank baik yang berkaitan dengan penyelenggaraan Teknologi Informasi maupun transaksi bisnis atau produk yang ditawarkan.

Bagian Ketiga

Penyelenggaraan Pemrosesan Transaksi oleh Pihak Penyedia Jasa

Pasal 20

(1) Penyelenggaraan pemrosesan transaksi oleh pihak penyedia jasa hanya dapat dilakukan sepanjang memenuhi prinsip kehati-hatian.
(2) Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak penyedia jasa di dalam negeri hanya dapat dilakukan sepanjang memenuhi persyaratan pada pasal 18 ayat (2) sampai dengan ayat (4);
(3) Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh pihak penyedia jasa di luar negeri hanya dapat dilakukan sepanjang memperoleh persetujuan dari Bank Indonesia.
(4) Persetujuan sebagaimana dimaksud pada ayat (3) dapat diberikan apabila bank memenuhi persyaratan sebagaimana dimaksud pada Pasal 18 ayat (2) sampai dengan ayat (4) dan pada Pasal 19 ayat (3) serta persyaratan tambahan sebagai berikut:
   a. Memperhatikan aspek perlindungan kepada nasabah;

b. Aktivitas yang pemrosesannya diserahkan kepada pihak penyedia jasa di luar negeri tidak merupakan aktivitas *inherent banking functions*;

c. Dokumen pendukung administrasi keuangan atas transaksi yang dilakukan di kantor Bank di Indonesia wajib dipelihara di kantor Bank di Indonesia.

d. Rencana Bisnis Bank menunjukkan adanya upaya untuk meningkatkan peran Bank bagi perkembangan perekonomian Indonesia.

Pasal 21

(1) Rencana penggunaan pihak penyedia jasa dalam penyelenggaraan Pusat Data (*Data Center), Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi wajib telah dimuat dalam Rencana Strategis Teknologi Informasi dan Rencana Bisnis Bank.

(2) Bank wajib melaporkan rencana penggunaan pihak penyedia jasa dalam penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi di dalam negeri kepada Bank Indonesia paling lambat 2 (dua) bulan sebelum penyelenggaraan kegiatan oleh pihak penyedia jasa tersebut efektif dioperasikan.

(3) Dalam hal terdapat rencana menyerahkan penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi kepada pihak penyedia jasa di luar negeri, Bank wajib menyampaikan permohonan persetujuan paling lambat 4 (empat) bulan sebelum penyelenggaraan kegiatan oleh pihak penyedia jasa tersebut efektif dioperasikan.

(4) Realisasi …

(4) Realisasi rencana penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi oleh pihak penyedia jasa wajib dilaporkan paling lambat 1 (satu) bulan sejak kegiatan tersebut efektif dioperasikan.

(5) Penyampaian rencana dan realisasi rencana sebagaimana dimaksud pada ayat (2), ayat (3) dan ayat (4) dilaksanakan dengan menggunakan format Laporan Perubahan Mendasar.

(6) Persetujuan atau penolakan atas permohonan sebagaimana dimaksud pada ayat (3) diberikan selambat-lambatnya 3 (tiga) bulan setelah dokumen permohonan diterima secara lengkap.

BAB V
ELECTRONIC BANKING

Pasal 22

(1) Bank yang menyelenggarakan kegiatan *Electronic Banking* wajib memenuhi ketentuan Bank Indonesia yang berlaku.

(2) Bank harus memberikan edukasi kepada nasabah mengenai produk *Electronic Banking* dan pengamanannya secara berkesinambungan.

Pasal 23

(1) Setiap rencana penerbitan produk *Electronic Banking* baru harus dimuat dalam Rencana Bisnis Bank.

(2) Setiap rencana penerbitan produk *Electronic Banking* yang bersifat transaksional wajib dilaporkan kepada Bank Indonesia paling lambat 2 (dua) bulan sebelum produk tersebut diterbitkan.

(3) Pelaporan rencana produk *Electronic Banking* sebagaimana dimaksud pada ayat (2) tidak berlaku bagi produk *Electronic Banking* sepanjang terdapat ketentuan Bank Indonesia yang secara khusus mengatur persyaratan persetujuan produk tersebut.

(4) Laporan rencana penerbitan produk sebagaimana dimaksud pada ayat (2) wajib dilengkapi dengan hal-hal sebagai berikut:

a. bukti-bukti kesiapan untuk menyelenggarakan *Electronic Banking* yang paling kurang memuat:

1) struktur organisasi yang mendukung termasuk pengawasan dari pihak manajemen;

2) kebijakan, sistem, prosedur dan kewenangan dalam penerbitan produk *Electronic Banking*;

3) kesiapan infrastruktur Teknologi Informasi untuk mendukung produk *Electronic Banking;*

4) hasil analisis dan identifikasi risiko terhadap risiko yang melekat pada produk *Electronic Banking*;

5) kesiapan penerapan manajemen risiko khususnya pengendalian pengamanan (*security control*) untuk memastikan terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authentication*), *non repudiation* dan ketersediaan (*availability*);

6) hasil analisis aspek hukum;

7) uraian sistem informasi akuntansi;

8) program perlindungan dan edukasi nasabah.

b. hasil analisis bisnis mengenai proyeksi produk baru 1 (satu) tahun kedepan.

(5) Penyampaian …

(5) Penyampaian pelaporan sebagaimana dimaksud dalam 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 praktek-praktek yang berlaku di dunia internasional.

(6) Dalam hal Teknologi Informasi yang digunakan dalam menyelenggarakan kegiatan *Electronic Banking* dilakukan oleh pihak penyedia jasa maka berlaku pula ketentuan sebagaimana diatur dalam Bab IV mengenai penyelenggaraan Teknologi Informasi oleh pihak penyedia jasa Teknologi Informasi.

(7) Realisasi rencana penerbitan produk *Electronic Banking* wajib dilaporkan paling lambat 1 (satu) bulan sejak rencana dilaksanakan dengan menggunakan format Laporan Perubahan Mendasar Teknologi Informasi.

BAB VI
PELAPORAN
Bagian Pertama
Laporan Penggunaan Teknologi Informasi
Pasal 24

(1) Bank wajib menyampaikan kembali Laporan Penggunaan Teknologi Informasi paling lambat 6 (enam) bulan sejak berlakunya Peraturan Bank Indonesia ini.

(2) Bank wajib menyampaikan Laporan Tahunan Penggunaan Teknologi Informasi paling lambat 1 (satu) bulan sejak akhir tahun pelaporan;

(3) Laporan Tahunan sebagaimana dimaksud pada ayat (2) untuk pertama kalinya disampaikan pada Januari 2009 untuk laporan tahun 2008.

Bagian …

Bagian Kedua

Laporan Perubahan Mendasar

Pasal 25

(1) Bank wajib menyampaikan Laporan Rencana Perubahan Mendasar Teknologi Informasi paling lambat 2 (dua) bulan sebelum perubahan tersebut efektif dioperasikan;

(2) Bank wajib menyampaikan Laporan Realisasi Rencana Perubahan Mendasar Teknologi Informasi paling lambat 1 (satu) bulan sejak perubahan tersebut efektif dioperasikan.

(3) Produk dan/atau aktivitas baru yang telah dilaporkan dalam Laporan Realisasi Rencana Perubahan Mendasar Teknologi Informasi tidak perlu dilaporkan dalam Laporan Produk dan Aktivitas Baru sebagaimana diatur dalam ketentuan Bank Indonesia mengenai manajemen risiko bank umum.

Bagian Ketiga

Laporan Lain

Pasal 26

(1) Bank wajib menyampaikan hasil audit Teknologi Informasi yang dilakukan pihak independen terhadap Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi yang penyelenggaraannya dilakukan oleh pihak penyedia jasa sebagaimana dimaksud dalam pasal 18 ayat (2) huruf b angka 7 paling lambat 2 (dua) bulan setelah audit selesai dilakukan.

(2) Bank wajib menyampaikan hasil penilaian penerapan manajemen risiko pada pihak penyedia jasa di luar negeri sebagaimana dimaksud dalam pasal 19 ayat (3) huruf e angka 3 paling lambat 1 (satu) bulan setelah akhir periode penilaian risiko.

(3) Bank …

(3) 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.

(4) Laporan sebagaimana dimaksud pada ayat (3) wajib disampaikan sesegera mungkin melalui e-mail atau telepon yang diikuti dengan laporan tertulis paling lambat 7 (tujuh) hari kerja setelah kejadian kritis dan/atau penyalahgunaan/kejahatan diketahui.

(5) Laporan tertulis sebagaimana dimaksud pada ayat (4) merupakan bagian dari Laporan kondisi yang berpotensi menimbulkan kerugian yang signifikan terhadap kondisi keuangan bank sebagaimana dimaksud dalam ketentuan tentang penerapan manajemen risiko bagi Bank Umum.

Bagian Keempat

Format dan Alamat Penyampaian Laporan

Pasal 27

Format dan petunjuk penyusunan laporan sebagaimana dimaksud dalam Pasal 24, Pasal 25 dan Pasal 26 diatur dalam Surat Edaran Bank Indonesia.

Pasal 28

Permohonan persetujuan penggunaan penyedia jasa di luar negeri sebagaimana dimaksud pada Pasal 19 dan Pasal 20 serta penyampaian laporan sebagaimana dimaksud dalam Pasal 24, Pasal 25 dan Pasal 26 dialamatkan kepada:

a. Direktorat Pengawasan Bank, Jl. MH Thamrin No.2, Jakarta 10350, bagi Bank yang berkantor pusat di wilayah kerja Kantor Pusat Bank Indonesia;

b. Kantor Bank Indonesia setempat, bagi Bank yang berkantor pusat di luar wilayah kerja Kantor Pusat Bank Indonesia.

BAB VII …

BAB VII

LAIN-LAIN

Pasal 29

(1) Bank Indonesia dapat melakukan pemeriksaan atau meminta Bank untuk melakukan pemeriksaan terhadap aspek-aspek terkait penggunaan Teknologi Informasi.

(2) Bank wajib menyediakan akses kepada Bank Indonesia untuk dapat melakukan pemeriksaan pada seluruh aspek terkait penyelenggaraan Teknologi Informasi baik yang diselenggarakan sendiri maupun yang diselenggarakan oleh pihak lain.

BAB VIII

SANKSI

Pasal 30

Bank yang tidak melaksanakan ketentuan sebagaimana ditetapkan dalam Peraturan Bank Indonesia ini dan ketentuan pelaksanaan terkait lainnya dapat dikenakan sanksi administratif sebagaimana dimaksud dalam Pasal 52 Undang Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang Undang Nomor 10 Tahun 1998, antara lain berupa:

a. teguran tertulis;
b. penurunan tingkat kesehatan berupa penurunan peringkat faktor manajemen dalam penilaian tingkat kesehatan;
c. pembekuan kegiatan usaha tertentu;
d. pencantuman anggota pengurus dalam daftar tidak lulus melalui mekanisme uji kepatutan dan kelayakan (*fit and proper test*).

Pasal 31 …

Pasal 31

Bank yang tidak memenuhi ketentuan pelaporan sebagaimana dimaksud dalam Pasal 21 ayat (2), ayat (3) dan ayat (4), Pasal 23 ayat (2) dan ayat (7), Pasal 24 dan Pasal 25 Peraturan Bank Indonesia ini dikenakan sanksi sesuai Pasal 52 Undang Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana diubah dengan Undang Undang Nomor 10 Tahun 1998, berupa:

a. kewajiban membayar sebesar Rp1.000.000,00 (satu juta rupiah) per hari keterlambatan per laporan;
b. kewajiban membayar 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.

Pasal 32

Bank yang menyampaikan laporan yang tidak sesuai dengan kondisi Bank yang sebenarnya dikenakan sanksi kewajiban membayar sebesar Rp50.000.000,00 (lima puluh juta rupiah) setelah Bank diberikan 2 (dua) kali surat teguran oleh Bank Indonesia dengan tenggang waktu 7 (tujuh) hari kerja untuk setiap teguran dan Bank tidak memperbaiki laporan dalam jangka waktu 7 (tujuh) hari kerja setelah surat teguran terakhir.

BAB IX

KETENTUAN PERALIHAN

Pasal 33

Bank yang telah memiliki kebijakan, prosedur dalam penggunaan Teknologi Informasi dan pedoman manajemen risiko penggunaan Teknologi Informasi wajib menyesuaikan dan menyempurnakannya paling lambat 12 (dua belas) bulan sejak berlakunya Peraturan Bank Indonesia ini.

Pasal 34 …

Pasal 34

Bank yang telah menggunakan pihak penyedia jasa Teknologi Informasi sebelum berlakunya Peraturan Bank Indonesia ini, wajib menyesuaikan perjanjian yang telah dibuat dengan ketentuan Peraturan Bank Indonesia ini paling lambat 12 (dua belas) bulan sejak berlakunya Peraturan Bank Indonesia ini.

Pasal 35

(1) Bank yang sebelum berlakunya Peraturan Bank Indonesia ini telah menyerahkan penyelenggaraan Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi kepada pihak penyedia jasa di luar negeri wajib menyampaikan permohonan persetujuan ulang untuk menyesuaikan dengan ketentuan dalam Peraturan Bank Indonesia ini paling lambat 12 (dua belas) bulan sejak berlakunya Peraturan Bank Indonesia ini.
(2) Dalam hal Bank tidak memperoleh persetujuan dari Bank Indonesia sebagaimana dimaksud pada ayat (1) maka Bank wajib menyampaikan laporan *action plan* kepada Bank Indonesia.
(3) *Action plan* sebagaimana dimaksud dalam ayat (2) disampaikan paling lambat 3 (tiga) bulan setelah jangka waktu sebagaimana dimaksud pada ayat (1) berakhir atau setelah permohonan Bank tidak disetujui.

Pasal 36

Bank yang belum memiliki Komite Pengarah Teknologi Informasi sebagaimana dimaksud dalam Pasal 7 wajib membentuk atau menyesuaikan komite tersebut dengan ketentuan dalam Peraturan Bank Indonesia ini paling lambat 12 (dua belas) bulan sejak berlakunya Peraturan Bank Indonesia ini.

BAB X …

BAB X

KETENTUAN PENUTUP

Pasal 37

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

Pasal 38

Dengan berlakunya Peraturan Bank Indonesia ini maka:

a. Surat Keputusan Direksi Bank Indonesia Nomor 27/164/KEP/DIR dan Surat Edaran Bank Indonesia Nomor 27/9/UPPB masing-masing tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank;
b. Surat Keputusan Direksi Bank Indonesia Nomor 31/175/KEP/DIR dan Surat Edaran Bank Indonesia Nomor 31/14/UPPB tanggal 22 Desember 1998 tentang Penyempurnaan Teknologi Sistem Informasi Bank dalam Menghadapi tahun 2000;
c. Peraturan Bank Indonesia Nomor 1/11/PBI/1999 tanggal 22 Desember 1999 tentang Fasilitas Khusus Dalam Rangka Mengatasi Kesulitan Pendanaan Jangka Pendek bagi Bank Umum yang disebabkan Masalah Komputer tahun 2000;
d. Surat Edaran Bank Indonesia Nomor 6/18/DPNP tanggal 20 April 2004 tentang Penerapan Manajemen Risiko pada Aktivitas Pelayanan Jasa Bank melalui Internet (*Internet Banking*);

dinyatakan tidak berlaku bagi Bank Umum.

Pasal 39 …

Pasal 39

Peraturan Bank Indonesia ini mulai berlaku pada tanggal 31 Maret 2008.

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

Ditetapkan di Jakarta
Pada tanggal 30 November 2007

a.n. GUBERNUR BANK INDONESIA

MIRANDA S. GOELTOM
DEPUTI GUBERNUR SENIOR

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2007 NOMOR 144
DPNP