OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA

SALINAN

PERATURAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 11 /POJK.03/2022

TENTANG

PENYELENGGARAAN TEKNOLOGI INFORMASI

OLEH BANK UMUM

DENGAN RAHMAT TUHAN YANG MAHA ESA

DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Menimbang : a. bahwa untuk mendukung kelangsungan operasional serta pelayanan bank kepada masyarakat, dibutuhkan pemanfaatan teknologi informasi oleh bank;

b. bahwa pemanfaatan teknologi informasi berpotensi meningkatkan eksposur risiko bagi bank sehingga bank perlu memperkuat tata kelola dalam penyelenggaraan teknologi informasi agar penyelenggaraan teknologi informasi bank dapat memberikan nilai tambah bagi bank melalui optimalisasi sumber daya untuk memitigasi risiko yang dihadapi oleh bank;

c. bahwa sejalan dengan dinamika pengaturan terkait penggunaan teknologi informasi serta perkembangan standar nasional dan internasional, perlu mengganti Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi

Informasi oleh Bank Umum sebagaimana telah diubah dengan Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.03/2020 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum;

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

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 PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Otoritas Jasa Keuangan ini, yang dimaksud dengan:

1. Bank Umum yang selanjutnya disebut sebagai Bank adalah bank yang melaksanakan kegiatan usaha secara konvensional atau melaksanakan kegiatan usaha berdasarkan prinsip syariah, yang dalam kegiatannya memberikan jasa dalam lalu lintas pembayaran, termasuk kantor cabang dari bank yang berkedudukan di luar negeri dan unit usaha syariah.
2. Teknologi Informasi yang selanjutnya disingkat TI adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
3. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
4. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.
5. Pusat Pemulihan Bencana adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia.
6. Rencana Pemulihan Bencana adalah dokumen yang berisikan rencana dan 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.

7. Direksi adalah organ Bank yang berwenang dan bertanggung jawab penuh atas pengurusan Bank untuk kepentingan Bank, sesuai dengan maksud dan tujuan Bank serta mewakili Bank, baik di dalam maupun di luar pengadilan sesuai dengan anggaran dasar bagi Bank yang berbadan hukum perseroan terbatas, organ atau pihak yang setara bagi Bank dengan bentuk badan hukum selain perseroan terbatas, atau pemimpin kantor cabang dan pejabat satu tingkat di bawah pemimpin kantor cabang bagi kantor cabang dari bank yang berkedudukan di luar negeri.
8. Dewan Komisaris adalah organ Bank yang bertugas melakukan pengawasan secara umum dan/atau khusus sesuai dengan anggaran dasar serta memberi nasihat kepada Direksi bagi Bank yang berbadan hukum perseroan terbatas, organ atau pihak yang setara bagi Bank dengan bentuk badan hukum selain perseroan terbatas, atau pihak yang ditunjuk untuk melaksanakan fungsi pengawasan bagi kantor cabang dari bank yang berkedudukan di luar negeri.

BAB II
TATA KELOLA TI BANK

Bagian Kesatu
Umum

Pasal 2

(1) Bank wajib menerapkan tata kelola TI yang baik dalam penyelenggaraan TI.
(2) Dalam menerapkan tata kelola TI yang baik sebagaimana dimaksud pada ayat (1), Bank mempertimbangkan faktor paling sedikit:
    a. strategi dan tujuan bisnis Bank;
    b. ukuran dan kompleksitas bisnis Bank;
    c. peran TI bagi Bank;

d. metode pengadaan sumber daya TI;
e. risiko dan permasalahan terkait TI;
f. praktik atau standar yang berlaku secara nasional maupun internasional; dan
g. ketentuan peraturan perundang-undangan.

(3) Dalam menerapkan tata kelola TI yang baik sebagaimana dimaksud pada ayat (1), Bank melakukan kegiatan paling sedikit:
a. evaluasi atas pilihan strategi, pengarahan atas strategi penyelenggaraan TI, dan pemantauan pencapaian strategi;
b. penyelarasan, perencanaan, dan pengorganisasian seluruh unit, strategi, dan kegiatan yang mendukung penyelenggaraan TI;
c. pendefinisian, akuisisi, dan implementasi atas solusi TI serta integrasinya dalam proses bisnis Bank;
d. penyediaan dukungan operasional layanan TI kepada pemangku kepentingan; dan
e. pemantauan kinerja dan kesesuaian penyelenggaraan TI dengan target kinerja intern, pengendalian intern, dan ketentuan peraturan perundang-undangan.

(4) Penerapan tata kelola TI yang baik sebagaimana dimaksud pada ayat (1) berlaku bagi seluruh unit dan/atau fungsi:
a. pengelola TI; dan
b. pengguna TI,
pada Bank.

Pasal 3

(1) Dalam menerapkan tata kelola TI, Bank wajib melakukan pemetaan, perencanaan, dan/atau penetapan atas aspek paling sedikit:
a. proses bisnis;
b. struktur organisasi;
c. kebijakan, standar, dan prosedur;

d. kebutuhan dan alur informasi pendukung proses bisnis;
e. sumber daya manusia pendukung;
f. budaya TI; dan
g. infrastruktur dan aplikasi.

(2) Bank memastikan terciptanya sinergi pada seluruh aspek sebagaimana dimaksud pada ayat (1).

(3) Bank wajib menerapkan kebijakan, standar, dan prosedur sebagaimana dimaksud pada ayat (1) huruf c secara konsisten dan berkesinambungan.

(4) Bank wajib melakukan kaji ulang dan penginian kebijakan, standar, dan prosedur sebagaimana dimaksud pada ayat (1) huruf c secara berkala.

Bagian Kedua
Penerapan Tata Kelola TI Bank

Pasal 4

Bank wajib menetapkan wewenang dan tanggung jawab yang jelas dari Direksi, Dewan Komisaris, dan pejabat pada setiap jenjang jabatan yang terkait dengan penerapan tata kelola TI.

Pasal 5

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

a. menetapkan rencana strategis TI;
b. menetapkan kebijakan, standar, dan prosedur terkait penyelenggaraan dan penggunaan TI yang memadai dan mengomunikasikan secara efektif, baik kepada satuan kerja penyelenggara maupun pengguna TI; dan
c. mengevaluasi tujuan strategis, mengarahkan pejabat eksekutif Bank, dan memantau seluruh kegiatan penyelenggaraan TI untuk memastikan:
    1. penerapan tata kelola TI sesuai dengan kebutuhan dan karakteristik Bank;

2. efektivitas dan efisiensi penyelenggaraan TI secara keseluruhan untuk memberikan manfaat yang optimal bagi Bank;
3. penerapan proses manajemen risiko dalam penyelenggaraan TI dilaksanakan secara efektif;
4. tersedianya sumber daya yang memadai terkait penyelenggaraan TI untuk mendukung bisnis Bank secara efektif dan efisien; dan
5. dukungan dan keterlibatan pemangku kepentingan dalam penerapan tata kelola TI.

Pasal 6

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

a. mengevaluasi, mengarahkan, dan memantau rencana strategis TI; dan
b. mengevaluasi, mengarahkan, dan memantau penerapan tata kelola TI.

Pasal 7

(1) Bank wajib memiliki komite pengarah TI.
(2) Komite pengarah TI sebagaimana dimaksud pada ayat (1) bertanggung jawab memberikan rekomendasi kepada Direksi paling sedikit terkait dengan:
    a. rencana strategis TI yang sejalan dengan rencana korporasi Bank;
    b. kebijakan, standar, dan prosedur TI;
    c. kesesuaian antara rencana pengembangan TI dan rencana strategis TI;
    d. kesesuaian antara pelaksanaan pengembangan TI dan rencana pengembangan TI;
    e. evaluasi atas efektivitas biaya TI terhadap pencapaian manfaat yang direncanakan;
    f. pemantauan atas kinerja TI dan upaya peningkatan kinerja TI;

g. upaya penyelesaian berbagai masalah terkait TI yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara TI secara efektif, efisien, dan tepat waktu; dan
h. kecukupan dan alokasi sumber daya terkait TI yang dimiliki Bank.

(3) Komite pengarah TI sebagaimana dimaksud pada ayat (1) paling sedikit beranggotakan:
a. direktur yang membawahkan satuan kerja penyelenggara TI;
b. direktur yang membawahkan satuan kerja manajemen risiko;
c. pejabat tertinggi yang memimpin satuan kerja penyelenggara TI; dan
d. pejabat tertinggi yang memimpin satuan kerja pengguna TI.

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

Pasal 8

(1) Bank wajib memiliki satuan kerja penyelenggara TI yang bertanggung jawab atas pengelolaan TI.

(2) Pengelolaan TI sebagaimana dimaksud pada ayat (1) paling sedikit berupa aktivitas:
a. perencanaan;
b. penyusunan atau pengembangan;
c. pengoperasian; dan
d. pemantauan,
atas kegiatan penyelenggaraan TI.

(3) Aktivitas pengelolaan TI sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan arahan yang ditetapkan oleh Direksi untuk mencapai tujuan bisnis Bank.

Pasal 9

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 2 ayat (1), Pasal 3 ayat (1), ayat (3), ayat (4), Pasal 4, Pasal 7 ayat (1), dan/atau Pasal 8 ayat (1), dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 2 ayat (1), Pasal 3 ayat (1), ayat (3), ayat (4), Pasal 4, Pasal 7 ayat (1), dan/atau Pasal 8 ayat (1), Bank dikenai sanksi administratif berupa:
   a. larangan untuk menerbitkan produk Bank baru;
   b. pembekuan kegiatan usaha tertentu; dan/atau
   c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 10

Ketentuan lebih lanjut mengenai penerapan tata kelola TI ditetapkan oleh Otoritas Jasa Keuangan.

BAB III

ARSITEKTUR TI BANK

Bagian Kesatu

Penyusunan Arsitektur TI Bank

Pasal 11

(1) Bank wajib memiliki arsitektur TI.

(2) Dalam menyusun arsitektur TI sebagaimana dimaksud pada ayat (1), Bank mempertimbangkan faktor paling sedikit:
   a. visi dan misi Bank;
   b. rencana korporasi Bank;
   c. proses dan kapabilitas bisnis Bank;
   d. tata kelola TI;

e. prinsip pengelolaan data, aplikasi, dan teknologi Bank;
f. ukuran dan kompleksitas bisnis Bank;
g. kemampuan permodalan Bank;
h. standar yang berlaku secara nasional maupun internasional; dan
i. ketentuan peraturan perundang-undangan.

(3) Arsitektur TI sebagaimana dimaksud pada ayat (1) disusun secara komprehensif meliputi proses:
a. perencanaan;
b. desain;
c. implementasi; dan
d. kontrol.

(4) Dalam hal terdapat perubahan pada faktor sebagaimana dimaksud pada ayat (2), Bank wajib melakukan penginian terhadap arsitektur TI.

(5) Ketentuan lebih lanjut mengenai penyusunan arsitektur TI ditetapkan oleh Otoritas Jasa Keuangan.

Bagian Kedua
Penyusunan Rencana Strategis TI Bank

Pasal 12

(1) Bank wajib memiliki rencana strategis TI yang mendukung rencana korporasi Bank.

(2) Rencana strategis TI sebagaimana dimaksud pada ayat (1) disusun untuk penyelenggaraan TI dalam jangka panjang sesuai periode rencana korporasi Bank.

(3) Ketentuan lebih lanjut mengenai penyusunan rencana strategis TI ditetapkan oleh Otoritas Jasa Keuangan.

Pasal 13

(1) Bank wajib menyampaikan rencana strategis TI sebagaimana dimaksud dalam Pasal 12 ayat (1) kepada Otoritas Jasa Keuangan paling lambat pada akhir bulan November tahun sebelum periode awal rencana strategis TI dimulai.

(2) Dalam hal terdapat kondisi yang secara signifikan memengaruhi sasaran dan strategi TI Bank sebagaimana dimuat dalam rencana strategis TI yang sedang berjalan, Bank dapat melakukan perubahan rencana strategis TI.

(3) Bank menyampaikan perubahan rencana strategis TI sebagaimana dimaksud pada ayat (2) kepada Otoritas Jasa Keuangan sewaktu-waktu dalam periode rencana strategis TI sebagaimana dimaksud dalam Pasal 12 ayat (2).

Pasal 14

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1), ayat (4), Pasal 12 ayat (1), dan/atau Pasal 13 ayat (1), dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1), ayat (4), Pasal 12 ayat (1), dan/atau Pasal 13 ayat (1), Bank dikenai sanksi administratif berupa:
   a. larangan untuk menerbitkan produk Bank baru;
   b. pembekuan kegiatan usaha tertentu; dan/atau
   c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

BAB IV
PENERAPAN MANAJEMEN RISIKO PENYELENGGARAAN TI BANK

Bagian Kesatu
Umum

Pasal 15

(1) Bank wajib menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI.

(2) Penerapan manajemen risiko sebagaimana dimaksud pada ayat (1) harus dilakukan secara terintegrasi dalam setiap tahapan penyelenggaraan TI.

(3) Dalam menerapkan manajemen risiko sebagaimana dimaksud pada ayat (1), Bank melakukan proses paling sedikit:
   a. identifikasi risiko;
   b. pengukuran risiko;
   c. pemantauan risiko; dan
   d. pengendalian risiko.

(4) Bank wajib memastikan kecukupan sistem informasi manajemen risiko dalam penyelenggaraan TI.

(5) Ketentuan lebih lanjut mengenai penerapan manajemen risiko dalam penyelenggaraan TI ditetapkan oleh Otoritas Jasa Keuangan.

Bagian Kedua
Pengamanan Informasi dalam
Penyelenggaraan TI Bank

Pasal 16

(1) Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dan efisien.

(2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) dilakukan terhadap aspek sumber daya manusia, proses, teknologi, dan fisik atau lingkungan, dalam penyelenggaraan TI secara menyeluruh.

(3) Penerapan pengamanan informasi sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan hasil penilaian terhadap risiko pada informasi yang dimiliki Bank.

(4) Ketentuan lebih lanjut mengenai pengamanan informasi ditetapkan oleh Otoritas Jasa Keuangan.

Pasal 17

(1) Bank wajib memastikan jaringan komunikasi yang disediakan oleh Bank telah memenuhi prinsip kerahasiaan, integritas, dan ketersediaan.
(2) Ketentuan lebih lanjut mengenai jaringan komunikasi ditetapkan oleh Otoritas Jasa Keuangan.

Pasal 18

(1) Bank wajib memiliki Rencana Pemulihan Bencana.
(2) Bank wajib memastikan Rencana Pemulihan Bencana sebagaimana dimaksud pada ayat (1) dapat dilaksanakan, sehingga kelangsungan operasional Bank tetap berjalan saat terjadi bencana dan/atau gangguan pada sarana TI 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, paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan melibatkan pengguna TI.
(4) Bank wajib melakukan kaji ulang Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(5) Ketentuan lebih lanjut mengenai Rencana Pemulihan Bencana ditetapkan oleh Otoritas Jasa Keuangan.

Pasal 19

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

Pasal 20

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 15 ayat (1), ayat (4), Pasal 16 ayat (1), Pasal 17 ayat (1), Pasal 18 ayat (1), ayat (2), ayat (3), ayat (4), dan/atau Pasal 19, dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 15 ayat (1), ayat (4), Pasal 16 ayat (1), Pasal 17 ayat (1), Pasal 18 ayat (1), ayat (2), ayat (3), ayat (4), dan/atau Pasal 19, Bank dikenai sanksi administratif berupa:

a. larangan untuk menerbitkan produk Bank baru;
b. pembekuan kegiatan usaha tertentu; dan/atau
c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

BAB V
KETAHANAN DAN KEAMANAN SIBER BANK

Pasal 21

(1) Bank wajib menjaga ketahanan siber.

(2) Untuk menjaga ketahanan siber sebagaimana dimaksud pada ayat (1), Bank melakukan proses paling sedikit:

a. identifikasi aset, ancaman, dan kerentanan;
b. pelindungan aset;
c. deteksi insiden siber; dan
d. penanggulangan dan pemulihan insiden siber.

(3) Bank memastikan proses untuk menjaga ketahanan siber sebagaimana dimaksud pada ayat (2) didukung dengan sistem informasi ketahanan siber yang memadai.

Pasal 22

(1) Bank wajib melakukan penilaian sendiri atas tingkat maturitas keamanan siber.

(2) Penilaian sendiri atas tingkat maturitas keamanan siber sebagaimana dimaksud pada ayat (1) dilakukan secara tahunan untuk posisi akhir bulan Desember.

(3) Bank dapat melakukan penginian penilaian sendiri atas tingkat maturitas keamanan siber sewaktu-waktu apabila diperlukan.

(4) Bank wajib menyampaikan hasil penilaian sendiri atas tingkat maturitas keamanan siber sebagaimana dimaksud pada ayat (1) kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.

Pasal 23

Bank wajib melakukan pengujian keamanan siber berdasarkan:

a. analisis kerentanan; dan

b. skenario.

Pasal 24

(1) Pengujian keamanan siber berdasarkan analisis kerentanan sebagaimana dimaksud dalam Pasal 23 huruf a wajib dilaksanakan secara berkala.

(2) Bank wajib menyampaikan hasil pengujian keamanan siber berdasarkan analisis kerentanan sebagaimana dimaksud pada ayat (1) kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.

Pasal 25

(1) Pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud dalam Pasal 23 huruf b wajib dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(2) Pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud pada ayat (1) paling sedikit mencakup:

a. penetapan tujuan, cakupan, dan skenario pengujian;

b. pelaksanaan pengujian;

c. evaluasi hasil pengujian; dan

d. penilaian terhadap efektivitas upaya mitigasi, respon, dan tindakan pemulihan Bank terhadap serangan siber.

(3) Bank wajib menyampaikan laporan hasil pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud pada ayat (1) kepada Otoritas Jasa Keuangan paling lama 10 (sepuluh) hari kerja setelah pengujian keamanan siber selesai dilaksanakan.

(4) Laporan hasil pengujian keamanan siber sebagaimana dimaksud pada ayat (3) paling sedikit mencakup:
a. ringkasan pelaksanaan pengujian;
b. pelajaran terpetik atau hasil observasi dari hasil pengujian; dan
c. rencana atau perbaikan yang telah dilakukan.

Pasal 26

(1) Bank wajib membentuk unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber Bank.

(2) Unit atau fungsi sebagaimana dimaksud pada ayat (1) bersifat independen terhadap fungsi pengelolaan TI.

Pasal 27

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 21 ayat (1), Pasal 22 ayat (1), ayat (4), Pasal 23, Pasal 24, Pasal 25 ayat (1), dan/atau Pasal 26 ayat (1), dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 21 ayat (1), Pasal 22 ayat (1), ayat (4), Pasal 23, Pasal 24, Pasal 25 ayat (1), dan/atau Pasal 26 ayat (1), Bank dikenai sanksi administratif berupa:
a. larangan untuk menerbitkan produk Bank baru;
b. pembekuan kegiatan usaha tertentu; dan/atau
c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 28

Ketentuan lebih lanjut mengenai ketahanan dan keamanan siber Bank ditetapkan oleh Otoritas Jasa Keuangan.

BAB VI

PENGGUNAAN PIHAK PENYEDIA JASA TI DALAM PENYELENGGARAAN TI BANK

Pasal 29

(1) Bank dapat menggunakan pihak penyedia jasa TI dalam penyelenggaraan TI.

(2) Bank yang menggunakan pihak penyedia jasa TI sebagaimana dimaksud pada ayat (1) wajib memiliki kemampuan dalam melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa TI.

(3) Bank wajib memiliki kebijakan dan prosedur dalam penggunaan pihak penyedia jasa TI sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
   a. proses identifikasi kebutuhan penggunaan pihak penyedia jasa TI;
   b. proses pemilihan pihak penyedia jasa TI;
   c. tata cara melakukan hubungan kerja sama dengan pihak penyedia jasa TI;
   d. proses manajemen risiko penggunaan pihak penyedia jasa TI; dan
   e. tata cara penilaian kinerja dan kepatuhan pihak penyedia jasa TI.

Pasal 30

(1) Bank dalam melakukan proses identifikasi kebutuhan penggunaan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 29 ayat (3) huruf a paling sedikit:
   a. meneliti potensi calon pihak penyedia jasa TI; dan
   b. menyusun kriteria pihak penyedia jasa TI yang dibutuhkan.

(2) Bank dalam melakukan proses pemilihan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 29 ayat (3) huruf b paling sedikit memperhatikan:
   a. kualifikasi dan kompetensi pihak penyedia jasa TI, termasuk sumber daya manusia yang dimiliki;
   b. analisis biaya dan manfaat dengan mengikutsertakan satuan kerja penyelenggara TI Bank;
   c. prinsip kehati-hatian dan manajemen risiko; dan
   d. prinsip hubungan kerja sama secara wajar jika pihak penyedia jasa TI merupakan pihak terkait dengan Bank.

(3) Bank dalam melakukan hubungan kerja sama dengan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 29 ayat (3) huruf c wajib memiliki perjanjian kerja sama dengan pihak penyedia jasa TI, dengan memperhatikan paling sedikit:
   a. kualifikasi dan kompetensi sumber daya manusia yang dimiliki pihak penyedia jasa TI;
   b. komitmen pihak penyedia jasa TI dalam menjaga kerahasiaan data dan/atau informasi Bank serta nasabah Bank;
   c. komitmen pihak penyedia jasa TI untuk menyampaikan hasil audit TI secara berkala yang dilakukan auditor independen atas penyediaan jasa TI kepada Bank;
   d. pengalihan sebagian kegiatan atau subkontrak oleh pihak penyedia jasa TI dilakukan atas persetujuan Bank yang dibuktikan dengan dokumen tertulis;
   e. mekanisme pelaporan kejadian kritis oleh pihak penyedia jasa TI kepada Bank;
   f. mekanisme penghentian perjanjian kerja sama jika terdapat penghentian perjanjian sebelum jangka waktu perjanjian berakhir;

g. pemenuhan ketentuan peraturan perundang-undangan atas penyediaan jasa TI oleh pihak penyedia jasa TI;

h. kesediaan pihak penyedia jasa TI untuk memenuhi kewajiban dan/atau persyaratan yang dimuat dalam perjanjian kerja sama; dan

i. kesediaan pihak penyedia jasa TI untuk memberikan akses kepada Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang untuk melakukan pemeriksaan terhadap kegiatan penyediaan jasa TI yang diberikan sesuai dengan ketentuan peraturan perundang-undangan.

(4) Proses manajemen risiko penggunaan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 29 ayat (3) huruf d meliputi:

a. tanggung jawab Bank atas penerapan manajemen risiko terkait penggunaan pihak penyedia jasa TI;

b. penyediaan Rencana Pemulihan Bencana yang teruji dan memadai; dan

c. penetapan dan pemantauan atas pemenuhan persyaratan keamanan data dan/atau informasi dalam kebijakan dan prosedur intern serta dalam perjanjian kerja sama.

(5) Bank dalam melakukan penilaian kinerja dan kepatuhan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 29 ayat (3) huruf e memperhatikan paling sedikit:

a. pemantauan dan evaluasi keandalan pihak penyedia jasa TI secara berkala terkait kinerja, reputasi pihak penyedia jasa TI, dan kelangsungan penyediaan layanan;

b. penerapan pengendalian TI secara memadai oleh pihak penyedia jasa TI, yang dibuktikan dengan hasil audit dan/atau penilaian yang dilakukan oleh pihak independen; dan

c. pemenuhan tingkat layanan sesuai dengan perjanjian tingkat layanan antara Bank dan pihak penyedia jasa TI.

Pasal 31

Dalam hal terdapat perubahan yang signifikan terhadap organisasi dari pihak penyedia jasa TI, Bank wajib melakukan penilaian ulang materialitas terhadap pihak penyedia jasa TI.

Pasal 32

(1) Dalam hal terdapat kondisi berupa:
   a. hasil penilaian ulang materialitas sebagaimana dimaksud dalam Pasal 31 menunjukkan bahwa kinerja pihak penyedia jasa TI berpotensi tidak berjalan dengan efektif;
   b. memburuknya kinerja penyelenggaraan TI oleh pihak penyedia jasa TI yang berpotensi menimbulkan dan/atau mengakibatkan dampak yang signifikan pada kegiatan usaha dan/atau operasional Bank;
   c. pihak penyedia jasa TI menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan;
   d. terdapat pelanggaran oleh pihak penyedia jasa TI terhadap ketentuan peraturan perundang-undangan mengenai rahasia Bank dan/atau data pribadi nasabah;
   e. terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan untuk pengawasan oleh Otoritas Jasa Keuangan; dan/atau
   f. terdapat kondisi lain yang menyebabkan terganggunya atau terhentinya penyediaan jasa TI dari pihak penyedia jasa TI kepada Bank,

   Bank wajib melakukan tindakan tertentu.

(2) Tindakan tertentu sebagaimana dimaksud pada ayat (1), paling sedikit:

a. melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi sebagaimana dimaksud pada ayat (1) diketahui oleh Bank;

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

c. melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah Bank menghentikan penggunaan pihak penyedia jasa TI sebelum berakhirnya jangka waktu perjanjian, dalam hal Bank memutuskan untuk menghentikan penggunaan pihak penyedia jasa TI.

(3) Dalam hal penggunaan pihak penyedia jasa TI atau rencana penggunaan pihak penyedia jasa TI menyebabkan atau diindikasikan akan menyebabkan kesulitan pengawasan yang dilakukan oleh Otoritas Jasa Keuangan, Otoritas Jasa Keuangan dapat:

a. memerintahkan Bank untuk menghentikan penggunaan pihak penyedia jasa TI sebelum berakhirnya jangka waktu perjanjian; atau

b. melarang rencana penggunaan pihak penyedia jasa TI oleh Bank.

(4) Dalam hal Bank akan menghentikan penggunaan pihak penyedia jasa TI, Bank wajib:

a. menyusun rencana penghentian penggunaan pihak penyedia jasa TI;

b. melakukan penilaian atas kelangsungan layanan dan data terkait dengan kegiatan yang diserahkan kepada pihak penyedia jasa TI serta pengujian atau simulasi terhadap kelangsungan kegiatan usaha dan/atau operasional Bank; dan

c. memastikan penghentian penggunaan pihak penyedia jasa TI tidak menimbulkan gangguan pada kegiatan usaha dan/atau operasional Bank.

Pasal 33

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 29 ayat (2), ayat (3), Pasal 30 ayat (3), Pasal 31, Pasal 32 ayat (1), dan/atau ayat (4), dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 29 ayat (2), ayat (3), Pasal 30 ayat (3), Pasal 31, Pasal 32 ayat (1), dan/atau ayat (4), Bank dikenai sanksi administratif berupa:
   a. larangan untuk menerbitkan produk Bank baru;
   b. pembekuan kegiatan usaha tertentu; dan/atau
   c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 34

Ketentuan lebih lanjut mengenai penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank ditetapkan oleh Otoritas Jasa Keuangan.

BAB VII
PENEMPATAN SISTEM ELEKTRONIK DAN
PEMROSESAN TRANSAKSI BERBASIS TI

Bagian Kesatu
Penempatan Sistem Elektronik

Pasal 35

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

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

(3) Kriteria Sistem Elektronik yang dapat ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud pada ayat (2), meliputi:

a. Sistem Elektronik yang digunakan untuk mendukung analisis terintegrasi dalam memenuhi ketentuan yang diterbitkan oleh otoritas negara asal Bank yang bersifat global, termasuk lintas negara;

b. Sistem Elektronik yang digunakan untuk manajemen risiko secara terintegrasi dengan kantor pusat Bank atau kantor induk atau kantor entitas utama di luar wilayah Indonesia;

c. Sistem Elektronik yang digunakan untuk penerapan anti pencucian uang dan pencegahan pendanaan terorisme secara terintegrasi dengan kantor pusat Bank atau kantor induk Bank di luar wilayah Indonesia;

d. Sistem Elektronik yang digunakan untuk pelayanan kepada nasabah secara global, yang memerlukan integrasi dengan Sistem Elektronik milik grup Bank di luar wilayah Indonesia;

e. Sistem Elektronik yang digunakan untuk manajemen komunikasi antara kantor pusat Bank dan kantor cabang, atau antara perusahaan anak dan perusahaan induk; dan/atau

f. Sistem Elektronik yang digunakan untuk manajemen intern Bank.

(4) Dalam hal terdapat kondisi yang mengganggu operasional Bank secara signifikan, Otoritas Jasa Keuangan dapat menentukan penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia selain kriteria

sebagaimana dimaksud pada ayat (3) untuk sementara waktu.

Pasal 36

(1) Bank dapat mengajukan permohonan izin sebagaimana dimaksud dalam Pasal 35 ayat (2) sepanjang Bank:
   a. memenuhi ketentuan sebagaimana dimaksud dalam Pasal 29 dan Pasal 30;
   b. menyampaikan hasil analisis risiko negara;
   c. memastikan penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia tidak mengurangi efektivitas pengawasan Otoritas Jasa Keuangan yang dibuktikan dengan surat pernyataan;
   d. memastikan bahwa informasi mengenai rahasia Bank hanya diungkapkan sepanjang memenuhi ketentuan peraturan perundang-undangan di Indonesia yang dibuktikan dengan perjanjian kerja sama antara Bank dan pihak penyedia jasa TI;
   e. memastikan bahwa perjanjian tertulis dengan pihak penyedia jasa TI memuat klausula pilihan hukum;
   f. menyampaikan surat pernyataan tidak keberatan dari otoritas pengawas pihak penyedia jasa TI di luar wilayah Indonesia bahwa Otoritas Jasa Keuangan dapat melakukan pemeriksaan terhadap pihak penyedia jasa TI;
   g. menyampaikan surat pernyataan bahwa Bank menyampaikan secara berkala hasil penilaian yang dilakukan kantor bank di luar wilayah Indonesia atas penerapan manajemen risiko pada pihak penyedia jasa TI;
   h. memastikan manfaat dari rencana penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah

Indonesia bagi Bank lebih besar daripada beban yang ditanggung oleh Bank;

i. menyampaikan rencana Bank untuk meningkatkan kemampuan sumber daya manusia Bank baik yang berkaitan dengan penyelenggaraan TI maupun transaksi bisnis atau produk yang ditawarkan; dan

j. menyampaikan rencana tindak penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di wilayah Indonesia bagi Bank yang akan menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 35 ayat (4).

(2) Otoritas Jasa Keuangan memberikan izin atau menolak permohonan izin penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 35 ayat (2) paling lama 3 (tiga) bulan setelah seluruh persyaratan dipenuhi oleh Bank dan dokumen permohonan diterima secara lengkap oleh Otoritas Jasa Keuangan.

(3) Bank wajib memastikan bahwa data yang digunakan dalam Sistem Elektronik yang ditempatkan pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia tidak digunakan untuk tujuan selain sebagaimana dimaksud dalam Pasal 35 ayat (3) atau Pasal 35 ayat (4).

(4) Dalam hal berdasarkan penilaian Otoritas Jasa Keuangan penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia:

a. tidak sesuai dengan permohonan izin penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia yang disampaikan kepada Otoritas Jasa Keuangan;

b. berpotensi mengurangi efektivitas pengawasan Otoritas Jasa Keuangan;
c. berpotensi berdampak negatif terhadap kinerja Bank; dan/atau
d. tidak sesuai dengan ketentuan peraturan perundang-undangan,

Otoritas Jasa Keuangan dapat meminta Bank untuk menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di wilayah Indonesia.

Pasal 37

Bank wajib memastikan Pusat Data dan Pusat Pemulihan Bencana sebagaimana dimaksud dalam Pasal 35 menjamin kelangsungan usaha Bank.

Pasal 38

Ketentuan lebih lanjut mengenai penempatan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana ditetapkan oleh Otoritas Jasa Keuangan.

Bagian Kedua
Pemrosesan Transaksi Berbasis TI

Pasal 39

(1) Bank wajib menyelenggarakan pemrosesan transaksi berbasis TI di wilayah Indonesia.
(2) Pemrosesan transaksi berbasis TI dapat dilakukan oleh pihak penyedia jasa TI di wilayah Indonesia.
(3) Penyelenggaraan pemrosesan transaksi berbasis TI oleh pihak penyedia jasa TI sebagaimana dimaksud pada ayat (2) dapat dilakukan sepanjang:
a. memenuhi prinsip kehati-hatian;
b. memenuhi ketentuan sebagaimana dimaksud dalam Pasal 29 dan Pasal 30; dan
c. memperhatikan aspek perlindungan nasabah.

(4) Pemrosesan transaksi berbasis TI oleh pihak penyedia jasa TI di luar wilayah Indonesia dapat dilakukan sepanjang Bank memperoleh izin dari Otoritas Jasa Keuangan.

(5) Bank dapat mengajukan permohonan izin sebagaimana dimaksud pada ayat (4) sepanjang:
   a. Bank memenuhi persyaratan sebagaimana dimaksud pada ayat (3);
   b. dokumen pendukung administrasi keuangan atas transaksi yang dilakukan di kantor Bank di Indonesia ditatausahakan di kantor Bank di Indonesia; dan
   c. rencana bisnis Bank menunjukkan adanya upaya untuk meningkatkan peran Bank bagi perkembangan perekonomian Indonesia.

(6) Otoritas Jasa Keuangan memberikan izin atau menolak permohonan izin pemrosesan transaksi berbasis TI oleh pihak penyedia jasa TI di luar wilayah Indonesia sebagaimana dimaksud pada ayat (4) paling lama 3 (tiga) bulan setelah seluruh persyaratan dipenuhi oleh Bank dan dokumen permohonan diterima secara lengkap oleh Otoritas Jasa Keuangan.

(7) Ketentuan lebih lanjut mengenai pemrosesan transaksi berbasis TI ditetapkan oleh Otoritas Jasa Keuangan.

Bagian Ketiga

Tata Cara Permohonan Izin dan Batas Waktu Pelaksanaan Setelah Memperoleh Izin

Pasal 40

(1) Permohonan izin sebagaimana dimaksud dalam Pasal 35 ayat (2) dan/atau Pasal 39 ayat (4) disampaikan kepada Otoritas Jasa Keuangan secara daring melalui sistem perizinan dan registrasi terintegrasi Otoritas Jasa Keuangan.

(2) Dalam hal sarana penyampaian sebagaimana dimaksud pada ayat (1) belum tersedia, penyampaian

dilakukan melalui sistem pelaporan Otoritas Jasa Keuangan untuk laporan tidak terstruktur kepada:

a. Departemen Pengawasan Bank terkait atau Kantor Regional Otoritas Jasa Keuangan di Jakarta, bagi Bank yang berkantor pusat di wilayah Provinsi Daerah Khusus Ibukota Jakarta atau Provinsi Banten; atau
b. Kantor Regional Otoritas Jasa Keuangan atau Kantor Otoritas Jasa Keuangan setempat, bagi Bank yang berkantor pusat di luar wilayah Provinsi Daerah Khusus Ibukota Jakarta atau Provinsi Banten.

Pasal 41

(1) Bank harus:
   a. menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 35 ayat (2); dan/atau
   b. mengimplementasikan pemrosesan transaksi berbasis TI oleh pihak penyedia jasa TI di luar wilayah Indonesia sebagaimana dimaksud dalam Pasal 39 ayat (4),

   paling lama 6 (enam) bulan sejak memperoleh izin dari Otoritas Jasa Keuangan.
(2) Apabila Bank tidak melaksanakan ketentuan sebagaimana dimaksud pada ayat (1) dalam jangka waktu 6 (enam) bulan sejak izin diperoleh dari Otoritas Jasa Keuangan, izin Otoritas Jasa Keuangan menjadi tidak berlaku.

Pasal 42

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 35 ayat (1), Pasal 36 ayat (3), Pasal 37, dan/atau Pasal 39 ayat (1), dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 35 ayat (1), Pasal 36 ayat (3), Pasal 37, dan/atau Pasal 39 ayat (1), Bank dikenai sanksi administratif berupa:
   a. larangan untuk menerbitkan produk Bank baru;
   b. pembekuan kegiatan usaha tertentu; dan/atau
   c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

BAB VIII
PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI DALAM PENYELENGGARAAN TI BANK

Bagian Kesatu
Pengelolaan Data oleh Bank

Pasal 43

(1) Bank wajib mengelola data secara efektif dalam pemrosesan data Bank untuk mendukung pencapaian tujuan bisnis Bank.
(2) Pengelolaan data secara efektif sebagaimana dimaksud pada ayat (1) memperhatikan paling sedikit:
   a. kepemilikan dan kepengurusan data;
   b. kualitas data;
   c. sistem pengelolaan data; dan
   d. sumber daya pendukung pengelolaan data.
(3) Ketentuan lebih lanjut mengenai pengelolaan data oleh Bank ditetapkan oleh Otoritas Jasa Keuangan.

Bagian Kedua
Pelindungan Data Pribadi oleh Bank

Pasal 44

(1) Bank wajib melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi.

(2) Dalam hal terdapat kondisi tertentu yang berpotensi meningkatkan risiko bagi pemilik data pribadi, Bank wajib melakukan penilaian dampak atas penerapan prinsip pelindungan data pribadi sebagaimana dimaksud pada ayat (1).

Pasal 45

(1) Dalam menerapkan pelindungan data pribadi pada kegiatan pertukaran data, Bank wajib menetapkan paling sedikit:
   a. klasifikasi data yang merupakan data pribadi;
   b. hak dan kewajiban para pihak yang terlibat dalam pertukaran data pribadi;
   c. perjanjian pertukaran data pribadi;
   d. sarana pertukaran data pribadi; dan
   e. keamanan data pribadi.

(2) Pertukaran data pribadi sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan persetujuan nasabah dan/atau calon nasabah yang dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 46

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 43 ayat (1), Pasal 44, dan/atau Pasal 45 ayat (1), dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 43 ayat (1), Pasal 44, dan/atau Pasal 45 ayat (1), Bank dikenai sanksi administratif berupa:
   a. larangan untuk menerbitkan produk Bank baru;
   b. pembekuan kegiatan usaha tertentu; dan/atau
   c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 47

Ketentuan lebih lanjut mengenai pelindungan data pribadi oleh Bank ditetapkan oleh Otoritas Jasa Keuangan.

BAB IX

PENYEDIAAN JASA TI OLEH BANK

Pasal 48

(1) Bank hanya dapat menyediakan jasa TI kepada lembaga jasa keuangan lain:
    a. yang diawasi oleh Otoritas Jasa Keuangan; dan/atau
    b. di luar wilayah Indonesia yang diawasi otoritas pengawas dan pengatur lembaga jasa keuangan setempat.
(2) Bank yang akan menyediakan jasa TI sebagaimana dimaksud pada ayat (1), wajib:
    a. memenuhi persyaratan penyediaan jasa TI tidak menjadi salah satu kegiatan pokok Bank;
    b. memenuhi prinsip kehati-hatian;
    c. memperhatikan analisis biaya dan manfaat;
    d. memenuhi prinsip hubungan kerja sama secara wajar; dan
    e. memenuhi ketentuan peraturan perundang-undangan.
(3) Bank wajib memperoleh izin Otoritas Jasa Keuangan untuk setiap rencana penyediaan jasa TI sebagaimana dimaksud pada ayat (1).
(4) Penyediaan jasa TI berupa aplikasi kepada lembaga jasa keuangan selain bank dapat dilakukan sepanjang:
    a. lembaga jasa keuangan pengguna jasa TI berada dalam satu grup atau kelompok dengan Bank; dan
    b. penggunaan aplikasi ditujukan untuk mendukung kegiatan operasional yang umum.

Pasal 49

(1) Permohonan izin sebagaimana dimaksud dalam Pasal 48 ayat (3) disampaikan kepada Otoritas Jasa Keuangan secara daring melalui sistem perizinan dan registrasi terintegrasi Otoritas Jasa Keuangan.

(2) Dalam hal sarana penyampaian sebagaimana dimaksud pada ayat (1) belum tersedia, penyampaian dilakukan melalui sistem pelaporan Otoritas Jasa Keuangan untuk laporan tidak terstruktur kepada:

a. Departemen Pengawasan Bank terkait atau Kantor Regional Otoritas Jasa Keuangan di Jakarta, bagi Bank yang berkantor pusat di wilayah Provinsi Daerah Khusus Ibukota Jakarta atau Provinsi Banten; atau

b. Kantor Regional Otoritas Jasa Keuangan atau Kantor Otoritas Jasa Keuangan setempat, bagi Bank yang berkantor pusat di luar wilayah Provinsi Daerah Khusus Ibukota Jakarta atau Provinsi Banten.

Pasal 50

(1) Bank harus melaksanakan rencana penyediaan jasa TI sebagaimana dimaksud dalam Pasal 48 ayat (3) paling lama 6 (enam) bulan sejak memperoleh izin dari Otoritas Jasa Keuangan.

(2) Apabila Bank tidak melaksanakan rencana penyediaan jasa TI sebagaimana dimaksud dalam Pasal 48 ayat (3) dalam jangka waktu 6 (enam) bulan sejak izin diperoleh dari Otoritas Jasa Keuangan, izin Otoritas Jasa Keuangan menjadi tidak berlaku.

Pasal 51

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 48 ayat (2) dan/atau ayat (3) dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum

memenuhi ketentuan sebagaimana dimaksud dalam Pasal 48 ayat (2) dan/atau ayat (3), Bank dikenai sanksi administratif berupa:

a. larangan untuk menerbitkan produk Bank baru;
b. pembekuan kegiatan usaha tertentu; dan/atau
c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 52

Ketentuan lebih lanjut mengenai penyediaan jasa TI oleh Bank ditetapkan oleh Otoritas Jasa Keuangan.

BAB X

PENGENDALIAN DAN AUDIT INTERN DALAM PENYELENGGARAAN TI BANK

Bagian Kesatu

Pengendalian Intern Bank dalam Penyelenggaraan TI

Pasal 53

(1) Bank wajib melaksanakan sistem pengendalian intern secara efektif dalam penyelenggaraan TI.
(2) Sistem pengendalian intern secara efektif sebagaimana dimaksud pada ayat (1) paling sedikit mencakup:
    a. pengawasan oleh manajemen dan penerapan budaya pengendalian;
    b. identifikasi dan penilaian risiko;
    c. kegiatan pengendalian dan pemisahan fungsi;
    d. dukungan sistem informasi, sistem akuntansi, dan sistem komunikasi; dan
    e. kegiatan pemantauan dan tindakan 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:
   a. kegiatan pemantauan secara terus menerus;
   b. pelaksanaan fungsi audit intern yang efektif dan menyeluruh; dan
   c. perbaikan terhadap penyimpangan yang diidentifikasi.

Bagian Kedua
Audit Intern dalam Penyelenggaraan TI

Pasal 54

(1) Bank melaksanakan fungsi audit intern TI yang efektif dan menyeluruh sebagaimana dimaksud dalam Pasal 53 ayat (4) huruf b sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern bagi bank umum.

(2) Untuk memastikan pelaksanaan audit intern TI yang efektif dan menyeluruh sebagaimana dimaksud dalam Pasal 53 ayat (4) huruf b, Bank wajib memastikan ketersediaan jejak audit atas seluruh kegiatan penyelenggaraan TI untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lain.

(3) Dalam hal Bank menggunakan jasa pihak ekstern dalam pelaksanaan audit intern TI, penggunaan jasa pihak ekstern dilakukan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern bagi bank umum.

(4) Bank wajib melaksanakan audit intern terhadap penyelenggaraan TI sesuai kebutuhan, prioritas, dan hasil analisis risiko atas penyelenggaraan TI, paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 55

(1) Bank wajib memiliki pedoman audit intern atas penyelenggaraan TI.

(2) Bank wajib melakukan kaji ulang terhadap fungsi audit intern atas penyelenggaraan TI paling sedikit 1 (satu) kali dalam 3 (tiga) tahun dengan menggunakan jasa pihak ekstern yang independen.

(3) Bank wajib menyampaikan kepada Otoritas Jasa Keuangan:
   a. hasil kaji ulang sebagaimana dimaksud pada ayat (2) sebagai bagian dari laporan hasil kaji ulang pihak ekstern yang independen; dan
   b. hasil audit intern TI sebagai bagian dari laporan pelaksanaan dan pokok-pokok hasil audit intern,

   sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan fungsi audit intern bagi bank umum.

Pasal 56

(1) Bank yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 53 ayat (1), Pasal 54 ayat (2), ayat (4), dan/atau Pasal 55, dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 53 ayat (1), Pasal 54 ayat (2), ayat (4), dan/atau Pasal 55, Bank dikenai sanksi administratif berupa:
   a. larangan untuk menerbitkan produk Bank baru;
   b. pembekuan kegiatan usaha tertentu; dan/atau
   c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 57

Ketentuan lebih lanjut mengenai pengendalian dan audit intern dalam penyelenggaraan TI Bank ditetapkan oleh Otoritas Jasa Keuangan.

BAB XI

PELAPORAN

Bagian Kesatu

Laporan Penyelenggaraan TI

Pasal 58

(1) Bank wajib melaporkan rencana pengembangan TI yang akan diimplementasikan 1 (satu) tahun ke depan paling lambat pada akhir bulan November sebelum tahun rencana pengembangan TI.
(2) Bank dapat melakukan perubahan rencana pengembangan TI yang telah disampaikan sebagaimana dimaksud pada ayat (1) paling banyak 1 (satu) kali, paling lambat pada akhir bulan Juni tahun berjalan.
(3) Bank dapat mengajukan perubahan rencana pengembangan TI selain dalam jangka waktu sebagaimana dimaksud pada ayat (2) sepanjang memenuhi pertimbangan tertentu dan mendapatkan persetujuan dari Otoritas Jasa Keuangan.
(4) Otoritas Jasa Keuangan dapat meminta Bank untuk melakukan penyesuaian terhadap perubahan rencana pengembangan TI sebagaimana dimaksud pada ayat (2).

Pasal 59

Bank wajib melaporkan kondisi terkini penyelenggaraan TI paling lama 15 (lima belas) hari kerja setelah akhir tahun pelaporan.

Bagian Kedua

Laporan Insidentil

Pasal 60

(1) Dalam hal terjadi insiden TI yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan

dan/atau mengganggu kelancaran operasional Bank, Bank wajib menyampaikan:

a. notifikasi awal paling lama 24 (dua puluh empat) jam setelah insiden TI diketahui; dan
b. laporan insiden TI paling lama 5 (lima) hari kerja setelah insiden TI diketahui.

(2) Notifikasi awal sebagaimana dimaksud pada ayat (1) huruf a disampaikan melalui sarana elektronik secara tertulis kepada Otoritas Jasa Keuangan berdasarkan informasi awal yang tersedia.

(3) Laporan insiden TI sebagaimana dimaksud pada ayat (1) huruf b merupakan bagian dari laporan kondisi yang berpotensi menimbulkan kerugian yang signifikan terhadap kondisi keuangan Bank sesuai dengan:

a. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum; atau
b. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

(4) Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal dan/atau laporan insiden TI dalam jangka waktu yang lebih cepat daripada jangka waktu sebagaimana dimaksud pada ayat (1), Bank wajib menyampaikan notifikasi awal dan/atau laporan insiden TI kepada Otoritas Jasa Keuangan pada saat yang bersamaan sesuai dengan ketentuan peraturan perundang-undangan otoritas lain dimaksud.

(5) Bank yang telah menyampaikan notifikasi awal dan/atau laporan insiden TI sebagaimana dimaksud pada ayat (4) dianggap telah memenuhi ketentuan sebagaimana dimaksud pada ayat (1) huruf a dan/atau huruf b.

Bagian Ketiga

Laporan Realisasi Penyelenggaraan TI Bank

Pasal 61

(1) Bank wajib menyampaikan laporan realisasi:
   a. penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia;
   b. pemrosesan transaksi berbasis TI di luar wilayah Indonesia; dan/atau
   c. kegiatan sebagai penyedia jasa TI.

(2) Laporan realisasi sebagaimana dimaksud pada ayat (1) disampaikan paling lama 3 (tiga) bulan setelah implementasi.

Bagian Keempat

Tata Cara Penyampaian Laporan

Pasal 62

(1) Bank menyampaikan laporan:
   a. hasil pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud dalam Pasal 25 ayat (3);
   b. rencana pengembangan TI sebagaimana dimaksud dalam Pasal 58 ayat (1);
   c. kondisi terkini penyelenggaraan TI sebagaimana dimaksud dalam Pasal 59;
   d. insiden TI sebagaimana dimaksud dalam Pasal 60 ayat (1) huruf b atau ayat (4); dan/atau
   e. realisasi sebagaimana dimaksud dalam Pasal 61,

   secara daring melalui sistem pelaporan Otoritas Jasa Keuangan.

(2) Bank yang melakukan pelanggaran terkait penyampaian laporan sebagaimana dimaksud pada ayat (1) dikenai sanksi administratif.

(3) Tata cara penyampaian laporan secara daring sebagaimana dimaksud pada ayat (1) dan pengenaan

sanksi administratif sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai pelaporan bank melalui sistem pelaporan Otoritas Jasa Keuangan.

Pasal 63

(1) Bank yang terlambat menyampaikan notifikasi awal insiden TI sebagaimana dimaksud dalam Pasal 60 ayat (1) huruf a atau ayat (4) dikenai sanksi administratif berupa teguran tertulis.

(2) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 60 ayat (1) huruf a atau ayat (4), Bank dikenai sanksi administratif berupa:
    a. larangan untuk menerbitkan produk Bank baru;
    b. pembekuan kegiatan usaha tertentu; dan/atau
    c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.

Pasal 64

Bank yang menyampaikan laporan secara tidak lengkap dikenai sanksi administratif atas kesalahan informasi sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai pelaporan bank melalui sistem pelaporan Otoritas Jasa Keuangan.

Pasal 65

Ketentuan lebih lanjut mengenai format pelaporan dan tata cara penyampaian laporan ditetapkan oleh Otoritas Jasa Keuangan.

BAB XII

PENILAIAN TINGKAT MATURITAS DIGITAL BANK

Pasal 66

(1) Bank wajib melakukan penilaian sendiri atas tingkat maturitas digital Bank secara berkala, paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(2) Tingkat maturitas digital Bank sebagaimana dimaksud pada ayat (1) mempertimbangkan seluruh aspek dalam penyelenggaraan TI.
(3) Bank wajib menyampaikan laporan hasil penilaian sendiri atas tingkat maturitas digital Bank sebagaimana dimaksud pada ayat (1) sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.
(4) Bank yang melanggar ketentuan sebagaimana dimaksud pada ayat (1) dan/atau ayat (3) dikenai sanksi administratif berupa teguran tertulis.
(5) Dalam hal Bank telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (4) dan belum memenuhi ketentuan sebagaimana dimaksud pada ayat (1) dan/atau ayat (3), Bank dikenai sanksi administratif berupa:
    a. larangan untuk menerbitkan produk Bank baru;
    b. pembekuan kegiatan usaha tertentu; dan/atau
    c. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan Bank.
(6) Ketentuan lebih lanjut mengenai penilaian sendiri atas tingkat maturitas digital Bank sebagaimana dimaksud pada ayat (1) ditetapkan oleh Otoritas Jasa Keuangan.

BAB XIII

KETENTUAN PERALIHAN

Pasal 67

Bank yang telah memiliki kebijakan, standar, dan prosedur dalam penyelenggaraan TI serta pedoman manajemen risiko penyelenggaraan TI harus menyesuaikan dengan ketentuan

dalam Peraturan Otoritas Jasa Keuangan ini paling lama 6 (enam) bulan sejak berlakunya Peraturan Otoritas Jasa Keuangan ini.

Pasal 68

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

Pasal 69

Bank harus menyesuaikan rencana strategis TI sesuai dengan ketentuan dalam Peraturan Otoritas Jasa Keuangan ini paling lambat akhir bulan November 2022.

BAB XIV
KETENTUAN PENUTUP

Pasal 70

Bank melaksanakan ketentuan terkait:

a. penilaian sendiri atas tingkat maturitas keamanan siber sebagaimana dimaksud dalam Pasal 22;
b. pengujian keamanan siber berdasarkan analisis kerentanan sebagaimana dimaksud dalam Pasal 24;
c. pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud dalam Pasal 25; dan
d. penilaian sendiri atas tingkat maturitas digital Bank sebagaimana dimaksud dalam Pasal 66,

untuk pertama kali setelah ditetapkan oleh Otoritas Jasa Keuangan.

Pasal 71

Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku, ketentuan pelaksanaan dari Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang

Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 267, Tambahan Lembaran Negara Republik Indonesia Nomor 5963) sebagaimana telah diubah dengan Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.03/2020 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 88, Tambahan Lembaran Negara Republik Indonesia Nomor 6486), dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Peraturan Otoritas Jasa Keuangan ini.

Pasal 72

Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku, Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 267, Tambahan Lembaran Negara Republik Indonesia Nomor 5963) sebagaimana telah diubah dengan Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.03/2020 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 88, Tambahan Lembaran Negara Republik Indonesia Nomor 6486), dicabut dan dinyatakan tidak berlaku.

Pasal 73

Peraturan Otoritas Jasa Keuangan ini mulai berlaku setelah 3 (tiga) bulan terhitung sejak tanggal diundangkan.

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

Ditetapkan di Jakarta
pada tanggal 6 Juli 2022

KETUA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

WIMBOH SANTOSO

Diundangkan di Jakarta
pada tanggal 7 Juli 2022

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

YASONNA H. LAOLY

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2022 NOMOR 5/OJK

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

PENJELASAN

ATAS

PERATURAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 11 /POJK.03/2022

TENTANG

PENYELENGGARAAN TEKNOLOGI INFORMASI

OLEH BANK UMUM

I. UMUM

Pemanfaatan TI bagi Bank merupakan suatu keniscayaan untuk mendukung kelangsungan operasional serta pelayanan Bank secara efektif dan efisien. Salah satu bentuk dukungan TI dalam operasional Bank yaitu otomasi proses kerja dengan pemanfaatan perangkat keras dan perangkat lunak tertentu. Dari sisi pelayanan kepada masyarakat, pemanfaatan TI diwujudkan melalui kemunculan inovasi layanan perbankan, antara lain *mobile banking* dan *internet banking* yang telah mempermudah masyarakat dalam melakukan transaksi.

Di sisi lain, seiring dengan perkembangan TI, industri perbankan Indonesia menghadapi tantangan yang baru dengan kemunculan industri jasa keuangan yang mengedepankan penyediaan kemudahan layanan keuangan dengan memanfaatkan TI. Hal ini menyebabkan persaingan di industri jasa keuangan semakin ketat. Dengan demikian, Bank semakin dituntut untuk melakukan peningkatan layanan kepada masyarakat melalui transformasi digital.

Dengan adanya tuntutan untuk melakukan transformasi digital, pemanfaatan TI untuk menunjang kegiatan operasional Bank serta penyediaan layanan kepada masyarakat juga semakin meningkat. Peningkatan pemanfaatan TI tersebut tentunya dapat menyebabkan peningkatan kompleksitas penyelenggaraan TI dalam berbagai aspek.

Hal tersebut berpotensi menimbulkan eksposur risiko baru bagi industri perbankan.

Beberapa contoh peningkatan eksposur risiko yang dihadapi oleh industri perbankan dengan peningkatan pemanfaatan TI yaitu:

a. peningkatan kerja sama layanan dengan pihak ketiga menyebabkan tingginya jumlah konektivitas sistem Bank dengan sistem pihak ketiga berpotensi meningkatkan celah keamanan yang berasal dari pihak ketiga sehingga dapat meningkatkan risiko terjadinya insiden siber Bank; dan
b. peningkatan penyediaan layanan yang mengedepankan personalisasi menyebabkan tingginya kebutuhan atas data olah Bank termasuk data pribadi nasabah sehingga berpotensi meningkatkan risiko kebocoran data pribadi nasabah.

Sehubungan dengan peningkatan risiko yang mungkin dihadapi, Bank perlu meningkatkan kematangan dalam penyelenggaraan TI melalui penerapan tata kelola TI yang baik. Hal ini bertujuan agar penyelenggaraan TI dapat memberikan nilai tambah dari investasi yang telah dikeluarkan Bank untuk mendukung tujuan bisnis Bank. Untuk dapat memberikan nilai tambah yang optimal, Bank harus mampu menangani risiko yang mungkin timbul dari pemanfaatan TI serta mengelola sumber daya yang dimiliki secara tepat guna.

Di samping itu, perkembangan TI yang cepat dan dinamis juga memengaruhi perubahan atas ketentuan maupun standar terkait penyelenggaraan TI, baik secara nasional maupun internasional. Dengan demikian, Bank perlu menyesuaikan diri dengan perkembangan ketentuan dan standar tersebut sesuai dengan kebutuhan dan kompleksitas dari penyelenggaraan TI Bank.

Sehubungan dengan hal tersebut dan untuk memperkuat seluruh aspek dalam penyelenggaraan TI serta memitigasi risiko yang mungkin timbul, perlu dilakukan penyusunan pengaturan tentang penyelenggaraan teknologi informasi oleh bank umum.

II. PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2

Ayat (1)

Penerapan tata kelola TI merupakan bagian dari penerapan tata kelola Bank secara umum. Tata kelola yang baik dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola bagi bank umum atau ketentuan peraturan perundang-undangan mengenai pelaksanaan *good corporate governance* bagi bank umum syariah dan unit usaha syariah.

Tata kelola TI diterapkan pada seluruh kegiatan yang berkaitan dengan penyelenggaraan TI antara lain manajemen risiko, ketahanan dan keamanan TI termasuk siber, pengelolaan data, penggunaan pihak penyedia jasa TI, penyediaan jasa TI oleh Bank, pengendalian intern, serta pengembangan dan perubahan TI.

Ayat (2)

Huruf a

Strategi dan tujuan bisnis Bank mencerminkan antara lain arah bisnis dan kebutuhan dari pemangku kepentingan.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Metode pengadaan sumber daya TI disesuaikan dengan kebutuhan dan kemampuan Bank, antara lain pengadaan secara mandiri, pengadaan dengan menggunakan pihak penyedia jasa TI, dan kombinasi antara keduanya.

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.

Huruf g

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 3

Ayat (1)

Huruf a

Dalam setiap kegiatan yang berkaitan dengan penyelenggaraan TI, Bank menentukan proses bisnis yang harus dilalui untuk mencapai tujuan strategis Bank.

Huruf b

Bank menetapkan penugasan dan tanggung jawab dalam setiap jabatan yang terkait pada setiap proses bisnis yang dimiliki Bank dalam penyelenggaraan TI sesuai dengan struktur organisasi Bank.

Huruf c

Kebijakan, standar, dan prosedur ditetapkan untuk seluruh proses bisnis yang dimiliki Bank dalam penyelenggaraan TI.

Huruf d

Cukup jelas.

Huruf e

Bank menetapkan dukungan jumlah sumber daya manusia yang cukup dengan keahlian dan kompetensi yang sesuai dalam penyelenggaraan TI.

Huruf f

Bank menetapkan budaya yang sesuai dengan pencapaian tujuan tata kelola TI.

Huruf g

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Bank menetapkan jangka waktu kaji ulang dan penginian kebijakan, standar, dan prosedur sesuai dengan kebutuhan

Bank dengan mempertimbangkan kondisi internal maupun eksternal Bank.

Pasal 4

Cukup jelas.

Pasal 5

Huruf a

Rencana strategis TI merupakan dokumen yang antara lain menggambarkan visi dan misi TI, strategi yang mendukung visi dan misi TI, dan prinsip utama yang menjadi acuan dalam penyelenggaraan TI untuk memenuhi kebutuhan bisnis serta mendukung rencana korporasi.

Huruf b

Cukup jelas.

Huruf c

Angka 1

Penerapan tata kelola TI yang sesuai dengan kebutuhan dan karakteristik Bank antara lain diwujudkan dengan:

a) kebijakan, standar, dan prosedur TI yang diterapkan secara efektif pada satuan kerja pengguna dan penyelenggara TI; dan

b) tersedianya sistem pengukuran kinerja proses penyelenggaraan TI yang antara lain dapat mendukung proses pemantauan terhadap implementasi strategi, mendukung penyelesaian proyek pengembangan TI, mengoptimalkan pendayagunaan sumber daya manusia dan investasi pada infrastruktur TI, serta meningkatkan kinerja proses penyelenggaraan TI dan kualitas layanan penyampaian hasil proses kepada pengguna TI.

Angka 2

Yang dimaksud dengan “memberikan manfaat yang optimal” adalah TI yang diselenggarakan Bank dapat mendukung perkembangan usaha Bank, pencapaian tujuan bisnis Bank, dan kelangsungan pelayanan terhadap nasabah Bank.

Angka 3

Proses manajemen risiko dalam penyelenggaraan TI termasuk manajemen risiko siber.

Angka 4

Tersedianya sumber daya yang memadai dapat ditunjukkan antara lain dengan terdapatnya:

a) kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan TI; dan

b) sistem pengelolaan pengamanan informasi yang efektif yang dikomunikasikan kepada satuan kerja pengguna dan penyelenggara TI.

Angka 5

Contoh keterlibatan pemangku kepentingan dapat berupa survei atas penggunaan TI dari satuan kerja pengguna TI.

Pasal 6

Cukup jelas.

Pasal 7

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Kesesuaian antara rencana pengembangan TI dan rencana strategis TI termasuk kesesuaian langkah untuk memitigasi risiko.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.

Huruf g

Cukup jelas.

Huruf h

Cukup jelas.

Ayat (3)

Struktur komite pengarah TI dapat disesuaikan dengan antara lain ukuran, kompleksitas bisnis, struktur kepemilikan, dan bentuk badan hukum Bank.

Ayat (4)

Cukup jelas.

Pasal 8

Cukup jelas.

Pasal 9

Cukup jelas.

Pasal 10

Cukup jelas.

Pasal 11

Ayat (1)

Yang dimaksud dengan “arsitektur TI” adalah dokumentasi strategis atas sumber daya TI Bank yang terorganisasi dan terintegrasi untuk mencapai dan mendukung tujuan bisnis Bank. Arsitektur TI antara lain berupa data, aplikasi, dan teknologi.

Ayat (2)

Huruf a

Cukup jelas.

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

Contoh ketentuan peraturan perundang-undangan yaitu ketentuan peraturan perundang-undangan mengenai informasi dan transaksi elektronik.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 12

Ayat (1)

Cukup jelas.

Ayat (2)

Periode rencana korporasi Bank sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai bank umum dan Peraturan Otoritas Jasa Keuangan mengenai bank umum syariah.

Ayat (3)

Cukup jelas.

Pasal 13

Ayat (1)

Contoh:

Rencana strategis TI periode tahun 2023 sampai dengan tahun 2027 disampaikan kepada OJK paling lambat akhir bulan November 2022.

Ayat (2)

Kondisi yang dapat memengaruhi sasaran dan strategi TI Bank antara lain perubahan rencana korporasi Bank atau perubahan ketentuan peraturan perundang-undangan mengenai penyelenggaraan teknologi informasi oleh bank.

Ayat (3)

Cukup jelas.

Pasal 14

Cukup jelas.

Pasal 15

Ayat (1)

Cakupan penerapan manajemen risiko secara efektif dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum atau Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

Manajemen risiko berlaku untuk seluruh penyelenggaraan TI antara lain:

a. keamanan siber;
b. pengelolaan data;
c. penggunaan pihak penyedia jasa TI; dan
d. penggunaan TI secara umum.

Ayat (2)

Tahapan penyelenggaraan TI antara lain proses perencanaan, pengadaan, pengembangan, operasional, pemeliharaan, penghentian, dan penghapusan sumber daya TI.

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

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 16

Ayat (1)

Pengamanan informasi ditujukan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikelola.

Contoh memastikan pengamanan informasi dilaksanakan secara efektif dan efisien antara lain dengan membangun dan memelihara sistem manajemen keamanan informasi.

Ayat (2)

Cukup jelas.

Ayat (3)

Dengan adanya penilaian terhadap risiko, Bank dapat menerapkan pengamanan informasi yang berbeda sesuai dengan risiko atas informasi tersebut.

Ayat (4)

Cukup jelas.

Pasal 17

Cukup jelas.

Pasal 18

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)

Hasil analisis dampak bisnis dikenal dengan istilah *business impact analysis*.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 19

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

Pasal 20

Cukup jelas.

Pasal 21

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang dimaksud dengan "sistem informasi ketahanan siber yang memadai" adalah sistem informasi yang dapat mendukung keseluruhan proses dalam menjaga ketahanan siber, sesuai dengan ukuran dan kompleksitas bisnis Bank.

Pasal 22

Ayat (1)

Dalam melakukan penilaian sendiri atas tingkat maturitas keamanan siber, Bank perlu melakukan analisis secara komprehensif dengan memperhatikan antara lain hasil penilaian terhadap pengujian keamanan siber.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 23

Cukup jelas.

Pasal 24

Ayat (1)

Contoh pengujian keamanan siber berdasarkan analisis kerentanan antara lain *penetration test*. Frekuensi pengujian keamanan siber berdasarkan analisis kerentanan dapat ditentukan berdasarkan beberapa faktor, seperti kekritisan sistem dan eksposur risiko terkait siber terhadap sistem.

Pengujian keamanan siber berdasarkan analisis kerentanan dilaksanakan secara berkala sesuai kebutuhan Bank.

Ayat (2)

Cukup jelas.

Pasal 25

Ayat (1)

Contoh pengujian keamanan siber berdasarkan skenario antara lain *cyber incident response*, *table-top exercise*, dan *cyber range exercise*.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Huruf a

Cukup jelas.

Huruf b

Pelajaran terpetik dikenal dengan istilah *lesson learned*.

Huruf c

Cukup jelas.

Pasal 26

Ayat (1)

Unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber Bank disesuaikan dengan ukuran dan kompleksitas bisnis Bank, termasuk alur pertanggungjawaban kepada Direksi.

Ayat (2)

Cukup jelas.

Pasal 27

Cukup jelas.

Pasal 28

Cukup jelas.

Pasal 29

Ayat (1)

Yang dimaksud dengan "menggunakan pihak penyedia jasa TI" adalah penggunaan jasa pihak lain dalam penyelenggaraan TI Bank secara berkesinambungan dan/atau dalam periode tertentu.

Yang dimaksud dengan pihak lain termasuk:

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

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

Contoh penyelenggaraan TI yang menggunakan pihak penyedia jasa TI antara lain penggunaan komputasi awan (*cloud computing*) sebagai Pusat Data dan/atau Pusat Pemulihan Bencana Bank.

Ayat (2)

Kemampuan Bank dalam melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa TI antara lain ditunjukkan dengan tersedianya sumber daya manusia yang memiliki pengetahuan atau kapabilitas mengenai jasa TI yang diberikan oleh pihak penyedia jasa TI.

Ayat (3)

Cukup jelas.

Pasal 30

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Bank memastikan pihak penyedia jasa TI memiliki tenaga ahli yang andal, dengan didukung oleh sertifikat keahlian secara akademis dan/atau secara profesional sesuai dengan keperluan penyelenggaraan TI.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Yang dimaksud dengan “pihak terkait dengan Bank” adalah pihak terkait sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai batas maksimum pemberian kredit dan penyediaan dana besar bagi bank umum atau Peraturan Otoritas Jasa Keuangan mengenai batas maksimum penyaluran dana dan penyaluran dana besar bagi bank umum syariah.

Ayat (3)

Huruf a

Cukup jelas.

Huruf b

Data dan/atau informasi Bank serta nasabah Bank merupakan aset yang harus dijamin keamanannya oleh

pihak penyedia jasa TI dengan cara dilindungi dari ancaman bahaya yang dapat mengganggu prinsip kerahasiaan, integritas, dan ketersediaan.

Informasi dalam hal ini termasuk informasi mengenai sistem dan perangkat yang digunakan untuk memproses, menyimpan, dan mengirimkan informasi.

Huruf c

Yang dimaksud dengan "secara berkala" adalah pelaksanaan audit sesuai dengan tingkat risiko yang akan diambil (*risk appetite*) oleh Bank terhadap jasa yang diberikan oleh pihak penyedia jasa TI.

Contoh cakupan audit yang dilakukan oleh auditor independen antara lain:

1. pengendalian fisik dan *logic* serta operasional Pusat Data dan/atau Pusat Pemulihan Bencana; dan
2. sistem aplikasi yang digunakan untuk memproses data Bank.

Huruf d

Cukup jelas.

Huruf e

Yang dimaksud dengan "kejadian kritis" adalah kejadian yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank.

Huruf f

Cukup jelas.

Huruf g

Termasuk ketentuan peraturan perundang-undangan terkait dengan pekerjaan yang diserahkan oleh Bank.

Huruf h

Cukup jelas.

Huruf i

Cukup jelas.

Ayat (4)

Huruf a

Tanggung jawab Bank atas penerapan manajemen risiko antara lain dilakukan dengan memastikan bahwa pihak

penyedia jasa TI menerapkan manajemen risiko pada kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa TI sesuai dengan Peraturan Otoritas Jasa Keuangan ini.

Huruf b

Yang dimaksud dengan "teruji dan memadai" adalah dapat menjaga kelangsungan operasional Bank saat terjadi bencana dan/atau gangguan pada sarana TI yang digunakan Bank.

Huruf c

Contoh cakupan keamanan data dan/atau informasi yang dipersyaratkan oleh Bank yaitu:

1. keamanan informasi organisasi;
2. pengelolaan akses;
3. manajemen enkripsi dan sandi;
4. keamanan jaringan dan operasi;
5. antarmuka pemrograman aplikasi (*Application Programming Interface*/API);
6. lokasi data; dan
7. kerahasiaan data pribadi nasabah Bank.

Ayat (5)

Huruf a

Yang dimaksud dengan "secara berkala" adalah pemantauan dan evaluasi keandalan pihak penyedia jasa TI sesuai dengan tingkat risiko yang akan diambil (*risk appetite*) oleh Bank terhadap jasa yang diberikan oleh pihak penyedia jasa TI.

Bank menggunakan prosedur kontrol dan pemantauan yang efektif untuk memantau kinerja pihak penyedia jasa TI dan mengelola risiko terkait kegiatan yang diserahkan oleh Bank, terutama jika kegiatan yang bersifat material terkonsentrasi pada satu perusahaan penyedia jasa TI.

Huruf b

Penerapan pengendalian TI secara memadai oleh pihak penyedia jasa TI memperhatikan antara lain pengamanan fisik dan pengamanan *logic*.

Pihak independen, bagi pihak penyedia jasa TI berupa bank yang berada dalam satu kelompok atau grup usaha, termasuk auditor intern.

Huruf c

Pemenuhan tingkat layanan dilakukan antara lain dengan memastikan penyelenggaraan TI dapat mendukung operasional Bank.

Perjanjian tingkat layanan dikenal dengan istilah *service level agreement.*

Pasal 31

Contoh perubahan yang signifikan antara lain perubahan kepemilikan atau kondisi keuangan pihak penyedia jasa TI, yang secara material dapat mengubah sifat, skala, dan kompleksitas risiko yang melekat pada penyediaan jasa TI.

Penilaian ulang materialitas dikenal dengan istilah *materiality reassesment*.

Pasal 32

Ayat (1)

Huruf a

Contoh kinerja pihak penyedia jasa TI berpotensi tidak berjalan dengan efektif antara lain ketidakmampuan pihak penyedia jasa TI untuk mendukung kebutuhan bisnis Bank.

Huruf b

Cukup jelas.

Huruf c

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

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Indikasi kesulitan pengawasan antara lain:

a. kesulitan dalam memperoleh akses terhadap data dan/atau informasi;
b. kesulitan dalam pelaksanaan pemeriksaan terhadap pihak penyedia jasa TI; dan
c. pihak penyedia jasa TI digunakan sebagai media untuk melakukan rekayasa data Bank dan/atau rekayasa keuangan Bank.

Ayat (4)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Bank antara lain memastikan bahwa semua data nasabah dan/atau calon nasabah telah dikembalikan atau dimusnahkan oleh pihak penyedia jasa TI.

Termasuk dalam kegiatan usaha Bank yaitu layanan kepada nasabah dengan memperhatikan aspek kerahasiaan, integritas, dan ketersediaan data.

Pasal 33

Cukup jelas.

Pasal 34

Cukup jelas.

Pasal 35

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Ketentuan yang diterbitkan oleh otoritas negara asal Bank untuk kantor cabang yaitu sesuai dengan kedudukan kantor pusat Bank di luar wilayah Indonesia, sedangkan untuk kantor subsidiari sesuai dengan kedudukan kantor induk atau kantor entitas utama berupa bank di luar wilayah Indonesia.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Pelayanan kepada nasabah secara global berupa Sistem Elektronik *front end* yang digunakan oleh Bank atau oleh nasabah untuk memperoleh layanan Bank yang disediakan secara global bagi seluruh nasabahnya, baik di wilayah Indonesia maupun di luar wilayah Indonesia, sebagai contoh *global cash management system*.

Sementara Sistem Elektronik yang digunakan untuk memproses laporan kepada otoritas dan *back end system* yang terakhir memproses data individu, akun, dan/atau transaksi nasabah, tetap ditempatkan di wilayah Indonesia.

Back end system antara lain:

1. *core banking system* yang digunakan untuk memproses data nasabah, giro, tabungan, deposito, dan kredit atau pembiayaan; dan
2. *back end system* yang digunakan untuk memproses kartu kredit, *sharia card*, *treasury*, pembiayaan perdagangan, dan *general ledger*.

Huruf e

Cukup jelas.

Huruf f

Sistem Elektronik yang digunakan untuk manajemen intern yaitu sistem yang digunakan Bank untuk keperluan intern, yang tidak terkait secara langsung

dengan pelayanan kepada nasabah dan/atau operasional Bank.

Sistem Elektronik yang digunakan untuk manajemen intern antara lain:

1. sistem kepegawaian;
2. sistem remunerasi; dan/atau
3. sistem audit intern.

Ayat (4)

Contoh kondisi yang mengganggu operasional Bank secara signifikan antara lain terhentinya layanan atau jasa dari pihak penyedia jasa TI serta tidak terdapat pihak penyedia jasa TI lain di wilayah Indonesia yang dapat memberikan layanan atau jasa yang serupa.

Sebelum berakhirnya masa penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia, Bank melakukan evaluasi untuk menentukan ketersediaan dan keandalan pihak penyedia Sistem Elektronik di wilayah Indonesia.

Pasal 36

Ayat (1)

Huruf a

Cukup jelas.

Huruf b

Risiko negara dikenal dengan istilah *country risk.*

Huruf c

Yang dimaksud dengan “tidak mengurangi efektivitas pengawasan Otoritas Jasa Keuangan” adalah tidak menimbulkan kesulitan bagi Otoritas Jasa Keuangan dalam memperoleh data dan/atau informasi yang diperlukan seperti adanya akses terhadap pangkalan data dan memiliki struktur pangkalan data dari setiap aplikasi yang digunakan.

Huruf d

Ketentuan peraturan perundang-undangan di Indonesia antara lain ketentuan peraturan perundang-undangan

mengenai persyaratan dan tata cara pemberian perintah atau izin tertulis membuka rahasia Bank.

Huruf e

Cukup jelas.

Huruf f

Surat pernyataan hanya disampaikan bagi pihak penyedia jasa TI yang memiliki otoritas pengawasan di bidang keuangan.

Huruf g

Kantor bank di luar wilayah Indonesia :

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

Surat pernyataan disampaikan termasuk jika bank memiliki kantor bank di wilayah yang sama dengan wilayah kedudukan penyedia jasa TI.

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.

Huruf j

Cukup jelas.

Ayat (2)

Yang dimaksud dengan “dokumen permohonan diterima secara lengkap” adalah diterimanya dokumen yang dipersyaratkan dalam Peraturan Otoritas Jasa Keuangan ini.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 37

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 pada Pusat Data dan Pusat Pemulihan Bencana.

Contoh langkah yang dapat dilakukan untuk menjamin kelangsungan usaha Bank antara lain Bank melakukan penilaian risiko atas Pusat Data dan Pusat Pemulihan Bencana, termasuk dengan mempertimbangkan eksposur risiko yang berbeda dari masing-masing Pusat Data dan Pusat Pemulihan Bencana.

Pusat Pemulihan Bencana termasuk Pusat Data yang beroperasi secara bersamaan dengan Pusat Data lainnya sehingga dapat saling menggantikan.

Pasal 38

Cukup jelas.

Pasal 39

Ayat (1)

Yang dimaksud dengan "pemrosesan transaksi berbasis TI" adalah kegiatan berupa penambahan, pengubahan, penghapusan, dan/atau otorisasi data yang dilakukan pada sistem aplikasi yang digunakan untuk memproses transaksi.

Ayat (2)

Cukup jelas.

Ayat (3)

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

Huruf a

Yang dimaksud dengan “prinsip kehati-hatian” antara lain pengelolaan risiko sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum atau Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah.

Huruf b

Cukup jelas.

Huruf c

Hubungan Bank dengan nasabah didasarkan atas perjanjian dengan memperhatikan antara lain Peraturan Otoritas Jasa Keuangan mengenai perlindungan konsumen dan Peraturan Otoritas Jasa Keuangan mengenai layanan pengaduan konsumen di sektor jasa keuangan.

Ayat (4)

Penyelenggaraan pemrosesan transaksi berbasis TI di luar wilayah Indonesia termasuk yang dilakukan pada kantor pusat atau kantor bank lain bagi kantor cabang dari bank yang berkedudukan di luar negeri atau kantor induk bagi Bank yang dimiliki lembaga keuangan asing.

Ayat (5)

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 atau pembiayaan dan dokumen pencairan kredit atau pembiayaan, *deal slip* dan *deal confirmation* dari 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 atau pembiayaan dan peningkatan pembiayaan ekspor-impor.

Ayat (6)

Cukup jelas.

Ayat (7)

Cukup jelas.

Pasal 40

Cukup jelas.

Pasal 41

Cukup jelas.

Pasal 42

Cukup jelas.

Pasal 43

Ayat (1)

Bentuk pemrosesan data antara lain perolehan, pendistribusian, pengolahan, pemeliharaan, penyimpanan, dan penghapusan data.

Ayat (2)

Huruf a

Kepemilikan data (*data ownership*) dan kepengurusan data (*data stewardship*) menjelaskan mengenai peran serta dan tanggung jawab masing-masing bagian dalam organisasi Bank yang terlibat dalam pengelolaan data.

Huruf b

Yang dimaksud dengan “kualitas data” adalah keandalan dan akurasi data antara lain untuk analisis bisnis dan pelaporan risiko.

Huruf c

Sistem pengelolaan data disesuaikan dengan kebutuhan dan kompleksitas Bank.

Sistem pengelolaan data antara lain:

1. arsitektur data;
2. pemodelan data (*data modelling* dan *design*);
3. penyimpanan dan operasi data (*data storage and operation*);
4. keamanan data;
5. integrasi dan interoperabilitas data;

6. pengelolaan dokumen dan konten;
7. *reference* dan *master data*;
8. *data warehouse* dan *business intelligence*; dan
9. metadata.

Huruf d

Sumber daya pendukung pengelolaan data antara lain berupa:

1. teknologi yang digunakan untuk mendukung sistem pengelolaan data; dan
2. sumber daya manusia yang kompeten untuk melakukan pengelolaan data.

Ayat (3)

Cukup jelas.

Pasal 44

Ayat (1)

Data pribadi dan prinsip pelindungan data pribadi sesuai dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi.

Ayat (2)

Contoh kondisi tertentu antara lain:

a. penggunaan teknologi baru;
b. pelacakan lokasi dan perilaku nasabah;
c. pemantauan atas lokasi fasilitas publik dalam skala besar; dan
d. pemrosesan data pribadi bersifat sensitif yang berkaitan dengan suku, agama, ras, dan antargolongan.

Yang dimaksud dengan "pemilik data pribadi" adalah nasabah dan/atau calon nasabah Bank.

Pasal 45

Ayat (1)

Huruf a

Cukup jelas.

Huruf b

Para pihak yang terlibat dalam pertukaran data pribadi antara lain:

1. pihak yang dapat memerintahkan pertukaran data pribadi;
2. pihak yang diwajibkan untuk membagikan data pribadi; dan
3. penerima data pribadi.

Huruf c

Penetapan perjanjian pertukaran data pribadi dilakukan termasuk untuk kondisi darurat.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Ayat (2)

Cukup jelas.

Pasal 46

Cukup jelas.

Pasal 47

Cukup jelas.

Pasal 48

Ayat (1)

Penyediaan jasa TI oleh Bank yaitu pemberian jasa berupa pemanfaatan infrastruktur TI milik Bank kepada lembaga jasa keuangan didasari dengan perjanjian kerja sama dan/atau sewa-menyewa di antara kedua belah pihak.

Contoh penyediaan jasa TI yaitu penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan aplikasi.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Prinsip kehati-hatian diterapkan dengan memperhatikan antara lain:

1. proses uji tuntas (*due diligence*) kepada pengguna jasa TI;

2. tata cara pengakhiran kerja sama (terminasi);
3. aspek keamanan; dan
4. kewajiban para pihak.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Huruf a

Yang dimaksud dengan “grup atau kelompok” adalah lembaga jasa keuangan yang memiliki keterkaitan kepemilikan dan/atau pengendalian.

Contoh: perusahaan anak dan *sister company*.

Huruf b

Penyediaan aplikasi tidak dimaksudkan bagi Bank untuk membangun aplikasi khusus bagi lembaga jasa keuangan selain bank.

Contoh aplikasi yang ditujukan untuk mendukung kegiatan operasional yang umum antara lain sistem remunerasi dan sistem kepegawaian.

Pasal 49

Cukup jelas.

Pasal 50

Cukup jelas.

Pasal 51

Cukup jelas.

Pasal 52

Cukup jelas.

Pasal 53

Ayat (1)

Prinsip umum pelaksanaan sistem pengendalian intern TI dilaksanakan sesuai dengan:

a. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum;
b. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank umum syariah dan unit usaha syariah; dan/atau
c. ketentuan Otoritas Jasa Keuangan mengenai pedoman standar sistem pengendalian intern bagi bank umum.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Termasuk pemantauan dan koreksi atas kesesuaian penyelenggaraan TI dengan perjanjian yang dimiliki serta ketentuan peraturan perundang-undangan.

Yang dimaksud dengan “pihak lain” adalah pihak intern Bank seperti unit atau fungsi kepatuhan Bank.

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 54

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Penggunaan jasa pihak ekstern untuk melaksanakan fungsi audit intern TI tidak mengurangi tanggung jawab pimpinan satuan kerja audit intern. Selain itu, penggunaan jasa pihak ekstern harus mempertimbangkan ukuran dan kompleksitas usaha Bank.

Dalam menggunakan jasa pihak ekstern untuk melaksanakan fungsi audit intern atas TI, Bank memperhatikan kerahasiaan data dan/atau informasi pada Bank yang akan diakses oleh pihak ekstern.

Ayat (4)

Cukup jelas.

Pasal 55

Ayat (1)

Penyelenggaraan TI termasuk untuk Bank yang menggunakan pihak penyedia jasa TI.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Cukup jelas.

Huruf b

Yang dimaksud dengan “hasil audit intern TI” adalah laporan hasil audit intern TI secara lengkap.

Pasal 56

Cukup jelas.

Pasal 57

Cukup jelas.

Pasal 58

Ayat (1)

Rencana pengembangan TI merupakan dokumen yang menjabarkan rincian rencana pengembangan TI untuk jangka waktu 1 (satu) tahun sebagaimana dimuat dalam rencana strategis TI Bank.

Ayat (2)

Cukup jelas.

Ayat (3)

Pertimbangan tertentu antara lain untuk mendukung implementasi kebijakan dan/atau ketentuan di sektor jasa keuangan dan/atau pemerintah untuk mendorong perkembangan perekonomian.

Ayat (4)

Cukup jelas.

Pasal 59

Laporan ini berisi kondisi penyelenggaraan TI Bank termasuk perubahan yang telah dilakukan selama 1 (satu) tahun pelaporan.

Pasal 60

Ayat (1)

Insiden TI yaitu kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI, berupa:

a. insiden siber; dan
b. insiden nonsiber.

Yang dimaksud dengan “kerugian” adalah kerugian keuangan dan/atau kerugian nonkeuangan. Contoh kerugian nonkeuangan yaitu pemberitaan negatif yang memengaruhi reputasi Bank.

Insiden siber yaitu ancaman siber, berupa upaya, kegiatan, dan/atau tindakan, yang mengakibatkan Sistem Elektronik tidak berfungsi sebagaimana mestinya.

Contoh insiden siber yaitu tidak berfungsinya Sistem Elektronik sebagaimana mestinya yang disebabkan oleh serangan siber antara lain peretasan, virus, *malware*,

ransomware, *web defacement*, dan *distributed denial of service attacks*.

Ayat (2)

Notifikasi awal disampaikan kepada satuan kerja pengawasan dari Bank.

Contoh sarana elektronik secara tertulis yaitu surat elektronik resmi.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 61

Ayat (1)

Laporan realisasi mencakup kajian pascaimplementasi (*post implementation review*).

Ayat (2)

Cukup jelas.

Pasal 62

Cukup jelas.

Pasal 63

Cukup jelas.

Pasal 64

Cukup jelas.

Pasal 65

Cukup jelas.

Pasal 66

Ayat (1)

Tingkat maturitas digital Bank mencerminkan pemenuhan terhadap seluruh aspek dalam penyelenggaraan TI sesuai

dengan Peraturan Otoritas Jasa Keuangan ini serta kesiapan Bank dalam mendukung transformasi digital.

Penilaian sendiri atas tingkat maturitas digital Bank secara berkala dilakukan dengan mempertimbangkan adanya perubahan kondisi intern dan ekstern Bank.

Contoh perubahan kondisi intern yaitu perubahan sasaran dan strategi bisnis Bank.

Contoh perubahan kondisi ekstern yaitu perkembangan TI.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Ayat (6)

Cukup jelas.

Pasal 67

Cukup jelas.

Pasal 68

Cukup jelas.

Pasal 69

Cukup jelas.

Pasal 70

Cukup jelas.

Pasal 71

Cukup jelas.

Pasal 72

Cukup jelas.

Pasal 73

Cukup jelas.

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 5/OJK