RINGKASAN
PERATURAN OTORITAS JASA KEUANGAN NOMOR 11/POJK.03/2022 TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

1. Latar Belakang

Berdasarkan Cetak Biru Transformasi Digital Perbankan yang memberikan gambaran mengenai arah kebijakan OJK dalam mendorong percepatan transformasi digital perbankan Indonesia, dibutuhkan penyempurnaan pengaturan yang mencakup aspek data, teknologi, manajemen risiko, kolaborasi, dan tatanan institusi. Untuk mendukung hal tersebut, OJK melakukan revolusi pengaturan yang diharapkan dapat lebih meningkatkan ketahanan dan kematangan operasional bank umum dalam seluruh aspek penyelenggaraan Teknologi Informasi (TI) melalui penerbitan POJK tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

2. Pokok Pengaturan

POJK tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum ini terdiri dari 14 Bab, dengan substansi pengaturan sebagai berikut:

A. BAB I – KETENTUAN UMUM

Bab ini berisi definisi yang digunakan dalam POJK ini yaitu definisi bank umum (Bank), TI, sistem elektronik, pusat data, pusat pemulihan bencana, rencana pemulihan bencana, direksi, dan dewan komisaris.

B. BAB II – TATA KELOLA TI BANK

Bab ini mengatur kewajiban Bank untuk menerapkan tata kelola TI dengan mempertimbangkan faktor tertentu. Selain itu, dijelaskan pula wewenang dan tanggung jawab dari direksi, dewan komisaris, komite pengarah TI, serta pejabat Bank terkait penerapan tata kelola TI.

C. BAB III – ARSITEKTUR TI BANK

Bab ini mengatur kewajiban Bank untuk:

1) memiliki arsitektur TI termasuk faktor yang perlu dipertimbangkan dalam penyusunannya; dan
2) memiliki rencana strategis TI jangka panjang yang mendukung rencana korporasi Bank. Rencana strategis TI disampaikan kepada OJK paling lambat pada akhir bulan November tahun sebelum periode awal rencana strategis TI dimulai.

D. BAB IV – PENERAPAN MANAJEMEN RISIKO PENYELENGGARAAN TI BANK

Bab ini mengatur kewajiban Bank terkait penerapan manajemen risiko dan pengamanan informasi dalam penyelenggaraan TI. Selain itu Bank juga wajib memiliki rencana pemulihan bencana serta melakukan uji coba dan kaji ulang atas rencana pemulihan bencana dimaksud paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

E. BAB V – KETAHANAN DAN KEAMANAN SIBER BANK Bab ini mengatur kewajiban Bank untuk:

1) menjaga ketahanan siber dengan melakukan proses:
   a) identifikasi aset, ancaman, dan kerentanan;
   b) pelindungan aset;
   c) deteksi insiden siber; dan
   d) penanggulangan pemulihan insiden siber, yang didukung dengan sistem informasi ketahanan siber yang memadai;
2) melakukan penilaian sendiri atas tingkat maturitas keamanan siber secara tahunan untuk posisi akhir bulan Desember;
3) melakukan pengujian keamanan siber; dan
4) membentuk unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber Bank.

F. BAB VI – PENGGUNAAN PIHAK PENYEDIA JASA TI DALAM PENYELENGGARAAN TI BANK

Bab ini mengatur hal-hal yang perlu diperhatikan dalam hal Bank menggunakan pihak penyedia jasa TI dalam penyelenggaraan TI. Bank wajib memiliki kebijakan dan prosedur dalam penggunaan pihak penyedia jasa TI yang paling sedikit memuat:

1) proses identifikasi kebutuhan penggunaan pihak penyedia jasa TI;
2) proses pemilihan pihak penyedia jasa TI;
3) tata cara melakukan hubungan kerja sama dengan pihak penyedia jasa TI;

4) proses manajemen risiko penggunaan pihak penyedia jasa TI; dan 5) tata cara penilaian kinerja dan kepatuhan pihak penyedia jasa TI.

G. BAB VII – PENEMPATAN SISTEM ELEKTRONIK DAN PEMROSESAN TRANSAKSI BERBASIS TI

Bab ini mengatur kewajiban penempatan sistem elektronik pada pusat data dan pusat pemulihan bencana di wilayah Indonesia serta pemrosesan transaksi berbasis TI di wilayah Indonesia. Bank dapat menempatkan sistem elektronik pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia serta pemrosesan transaksi berbasis TI di luar wilayah Indonesia berdasarkan kriteria dan persyaratan tertentu dengan terlebih dahulu memperoleh izin dari OJK.

H. BAB VIII – PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI DALAM PENYELENGGARAAN TI BANK

Bab ini mengatur kewajiban Bank untuk:

1) mengelola data secara efektif dalam pemrosesan data Bank dengan memperhatikan paling sedikit:
   a) kepemilikan dan kepengurusan data;
   b) kualitas data;

c) sistem pengelolaan data; dan

d) sumber daya pendukung pengelolaan data;

2) melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi.

I. BAB IX – PENYEDIAAN JASA TI OLEH BANK

Bab ini mengatur hal-hal yang terkait dengan penyediaan jasa TI oleh Bank.

1) Bank hanya dapat menyediakan jasa TI kepada lembaga jasa keuangan lain yang diawasi oleh OJK dan/atau lembaga jasa keuangan lain di luar wilayah Indonesia yang diawasi oleh otoritas pengawas dan pengatur lembaga jasa keuangan setempat.
2) Bank wajib memperoleh izin atas rencana penyediaan jasa TI.
3) Penyediaan jasa TI berupa aplikasi kepada lembaga jasa keuangan selain bank dapat dilakukan sepanjang lembaga jasa keuangan dimaksud berada dalam satu grup atau kelompok dengan Bank dan penggunaan aplikasi ditujukan untuk mendukung kegiatan operasional yang umum.

J. BAB X – PENGENDALIAN DAN AUDIT INTERN DALAM PENYELENGGARAAN TI BANK

Bab ini mengatur kewajiban Bank untuk:

1) melaksanakan sistem pengendalian intern secara efektif dalam penyelenggaraan TI;
2) melaksanakan audit intern terhadap penyelenggaraan TI paling sedikit 1 (satu) kali dalam 1 (satu) tahun; dan
3) memiliki pedoman audit intern atas penyelenggaraan TI; serta
4) melakukan kaji ulang terhadap fungsi audit intern paling sedikit 1 (satu) kali dalam 3 (tiga) tahun dengan menggunakan jasa pihak ekstern yang independen.

K. BAB XI – PELAPORAN

Bab ini mengatur penyampaian dokumen kepada OJK antara lain:

1) rencana pengembangan TI;
2) laporan kondisi terkini penyelenggaraan TI;
3) notifikasi awal dan laporan insiden TI; dan
4) laporan realisasi penyelenggaraan TI Bank.

Penyampaian laporan dilakukan secara daring dengan memanfaatkan sistem elektronik milik OJK.

L. BAB XII – PENILAIAN TINGKAT MATURITAS DIGITAL BANK Bab ini mengatur kewajiban Bank untuk:

1) melakukan penilaian sendiri atas tingkat maturitas digital Bank paling sedikit 1 (satu) kali dalam 1 (satu) tahun; dan
2) menyampaikan laporan hasil penilaian sendiri atas tingkat maturitas digital Bank kepada OJK.

M. BAB XIII - KETENTUAN PERALIHAN Bank harus menyesuaikan:

1) kebijakan, standar, dan prosedur dalam penyelenggaraan TI, serta pedoman manajemen risiko penyelenggaraan TI;
2) perjanjian penggunaan pihak jasa TI; dan/atau
3) rencana strategis TI, sesuai dengan POJK ini.

N. BAB XIV – KETENTUAN PENUTUP

1) Bank melaksanakan ketentuan terkait:
   a) penilaian tingkat maturitas keamanan siber;
   b) pengujian keamanan siber; dan
   c) penilaian sendiri atas tingkat maturitas digital Bank, untuk pertama kali setelah ditetapkan oleh OJK.
2) POJK ini mulai berlaku 3 (tiga) bulan terhitung sejak tanggal diundangkan.

-----∞-----