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.

-----∞-----

TANYA JAWAB

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

1. **Apa latar belakang penerbitan POJK ini?**
   Perkembangan Teknologi Informasi (TI) memberikan tantangan baru bagi industri perbankan di Indonesia, khususnya dengan kemunculan industri jasa keuangan yang mengedepankan penyediaan kemudahan layanan keuangan dengan memanfaatkan TI, seperti *fintech*. Hal ini menuntut bank untuk melakukan peningkatan layanan kepada masyarakat melalui transformasi digital. Transformasi digital tidak lepas dari penyelenggaraan TI, sementara itu penyelenggaraan TI berpotensi meningkatkan eksposur risiko bank, termasuk risiko terkait keamanan siber. Untuk itu, bank perlu meningkatkan kematangan dalam penyelenggaraan TI melalui penerapan tata kelola TI yang baik, sehingga penyelenggaraan TI mampu memberikan nilai tambah dalam mendukung tujuan bisnis bank secara optimal. OJK memberikan dukungan kepada bank melalui penerbitan POJK ini yang memberikan pedoman dan pengaturan terkait dengan aspek TI yang perlu dipenuhi oleh bank.

2. **Apa saja hal-hal yang diatur dalam POJK ini?**
   POJK ini mengatur mengenai seluruh aspek dalam penyelenggaraan TI oleh bank, yang mencakup:
   a. tata kelola TI;
   b. arsitektur TI dan rencana strategis TI;
   c. penerapan manajemen risiko dalam penyelenggaraan TI;
   d. ketahanan dan keamanan siber;
   e. penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI;
   f. penempatan sistem elektronik dan pemrosesan transaksi berbasis TI;
   g. pengelolaan data dan pelindungan data pribadi dalam penyelenggaraan TI;
   h. penyediaan jasa TI oleh bank;
   i. pengendalian dan audit intern dalam penyelenggaraan TI;
   j. pelaporan;
   k. penilaian tingkat maturitas digital; dan
   l. ketentuan peralihan.

3. **Bagaimana pelaporan rencana strategis TI sesuai POJK ini, serta perlakuan terhadap rencana strategis TI yang sudah dimiliki bank?**
   Rencana strategis TI disusun oleh bank untuk penyelenggaraan TI dalam jangka panjang sesuai dengan periode rencana korporasi bank. Apabila rencana korporasi bank berlaku selama 5 (lima) tahun maka rencana strategis TI juga disusun untuk periode 5 (lima) tahun dalam rangka mendukung rencana korporasi tersebut. Sebagai contoh, khusus untuk tahun 2022, apabila bank telah memiliki rencana korporasi untuk periode tahun 2022 – 2026, maka dalam hal rencana strategis TI yang dimiliki bank per tahun 2022 menggunakan periode yang berbeda (contoh 2022-2024), bank perlu menyesuaikan rencana

strategis TI dimaksud menjadi rencana strategis TI tahun 2022-2026 dan disampaikan paling lambat pada akhir bulan November 2022.

4. **Apakah bank dapat menggunakan layanan *cloud computing*?**
   Ya, bank dapat menggunakan layanan *cloud computing* dalam penyelenggaraan TI bank. Dalam hal bank menggunakan layanan *cloud computing*, maka penyedia jasa *cloud computing* bertindak sebagai pihak penyedia jasa TI sebagaimana diatur dalam POJK ini. Dengan demikian bank wajib melaksanakan ketentuan dalam POJK ini yang terkait dengan penggunaan pihak penyedia jasa TI. Selanjutnya, dalam hal bank menggunakan penyedia jasa *cloud computing* yang berada di luar wilayah Indonesia, pengaturan yang terkait dengan penempatan sistem elektronik di luar wilayah Indonesia dalam POJK ini tetap berlaku dan wajib dipenuhi.

5. **Bagaimana proses perizinan penempatan sistem elektronik pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia?**
   Penempatan sistem elektronik pada pusat data dan/atau pusat pemulihan bencana termasuk sebagai pengembangan TI, oleh karena itu bank perlu mencantumkan rencana penempatan sistem elektronik tersebut dalam rencana pengembangan TI. Kemudian, bank mengajukan permohonan izin penempatan sistem elektronik kepada OJK. Selanjutnya, setelah seluruh persyaratan dipenuhi oleh Bank dan dokumen permohonan izin diterima secara lengkap oleh OJK maka OJK memberikan izin atau menolak permohonan izin dalam jangka waktu paling lama 3 (tiga) bulan.

   Bank harus melaksanakan rencana penempatan sistem elektronik tersebut paling lama 6 (bulan) sejak memperoleh izin dari OJK. Apabila bank belum melaksanakan rencana penempatan sistem elektronik dalam jangka waktu 6 (enam) bulan sejak izin diperoleh maka izin tersebut menjadi tidak berlaku.

6. **Apakah *core banking system* dapat ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia?**
   Core banking system bukan merupakan salah satu sistem elektronik yang memenuhi kriteria sistem elektronik yang dapat ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia sesuai dengan POJK ini. Dengan demikian, *core banking system* tetap wajib ditempatkan pada pusat data dan pusat pemulihan bencana di Indonesia.

7. **Apabila suatu sistem elektronik memiliki satu atau lebih fungsi/modul yang sesuai dengan kriteria sistem elektronik yang dapat ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia, apakah sistem elektronik tersebut dapat ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia?**
   Suatu sistem elektronik dapat terdiri atas beberapa fungsi/modul. Apabila salah satu atau lebih fungsi/modul yang ada dalam sistem elektronik memenuhi kriteria sistem elektronik yang dapat ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia, tidak berarti sistem elektronik tersebut bisa ditempatkan di luar wilayah Indonesia.

Jika bank tetap bermaksud untuk menempatkan fungsi/modul tersebut pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia, bank harus dapat memisahkan fungsi/modul tersebut menjadi sistem elektronik tersendiri. Dengan demikian, hanya fungsi/modul yang telah dipisahkan tersebut yang dapat ditempatkan pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia, dengan persetujuan OJK.

8. **Apakah bank memerlukan izin OJK dalam melakukan pemrosesan transaksi yang dilakukan di wilayah Indonesia?**
   Tidak, pemrosesan transaksi di wilayah Indonesia tidak memerlukan izin OJK, namun demikian bank tetap mencantumkan rencana pemrosesan transaksi di Indonesia dalam laporan rencana pengembangan TI yang disampaikan paling lambat setiap akhir bulan November.

9. **Apakah terdapat batasan waktu bagi bank untuk menempatkan sistem elektronik pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia dalam hal terdapat kondisi yang mengganggu operasional Bank secara signifikan sebagaimana dimaksud dalam Pasal 35 ayat (4)?**
   Dalam POJK ini tidak diatur mengenai batasan waktu dimaksud, penentuan batasan waktu merupakan hal yang perlu dianalisis oleh bank sebelum mengajukan izin penempatan sistem elektronik pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia sebagaimana diatur dalam Pasal 35 ayat (4) kepada OJK.

10. **Apakah bank diperbolehkan untuk menyediakan jasa TI kepada pihak lain?**
    Penyelenggaraan TI tentu membutuhkan infrastruktur TI yang mendukung. Sementara itu, dalam penyediaan infrastruktur TI terdapat kemungkinan adanya kapasitas yang belum terpakai secara optimal (*idle*). Hal ini berdampak terhadap efisiensi penyelenggaraan TI bank. Penyediaan jasa TI oleh bank diperbolehkan sepanjang hal tersebut bertujuan untuk mengoptimalkan infrastruktur TI yang telah dimiliki oleh bank. Dengan demikian, penyediaan jasa TI tidak menjadi kegiatan pokok dari bank tersebut. Adapun penyediaan jasa TI oleh bank terbatas pada lembaga jasa keuangan.

11. **Dalam hal Bank A menyediakan jasa TI kepada perusahaan anak berupa bank umum yaitu Bank B, bagaimana mekanisme penyelenggaraan TI bagi kedua bank dimaksud?**
    Dalam hal ini Bank A bertindak sebagai penyedia jasa TI, sehingga berdasarkan Pasal 48 POJK ini, Bank A wajib memperoleh izin dari OJK terlebih dahulu. Di sisi lain, Bank B menggunakan jasa Bank A sebagai pihak penyedia jasa TI sehingga Bank B perlu memperhatikan ketentuan sebagaimana diatur dalam Bab VI POJK ini.

12. **Apabila bank mengembangkan TI bagi nasabah dalam rangka penyediaan produk bank, apakah bank diwajibkan untuk memenuhi ketentuan sebagaimana dimaksud dalam Bab IX POJK ini?**
    Tidak, pengembangan TI bagi nasabah tidak termasuk dalam cakupan pengaturan pada Bab IX POJK ini mengingat penyediaan jasa TI dimaksud

merupakan bagian dari produk Bank yang mekanisme perizinannya mengikuti ketentuan POJK No.13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum.

Contoh penyediaan TI bagi nasabah dalam rangka produk bank adalah *cash management system*. Bank mengembangkan suatu aplikasi bagi nasabah untuk dapat mengakses layanan *cash management system* yang diberikan oleh bank.

13. Apa saja yang termasuk sebagai insiden siber?

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* (DDOS) *attack*s.

14. Bagaimana pelaporan insiden siber dalam hal terdapat otoritas lain yang juga mewajibkan pelaporan dimaksud?

Sesuai dengan POJK ini, dalam hal terdapat insiden TI, termasuk dalam hal ini insiden siber, bank wajib menyampaikan notifikasi awal paling lama 24 (dua puluh empat) jam dan laporan insiden TI kepada OJK paling lama 5 (lima) hari kerja, setelah insiden TI diketahui. Apabila terdapat otoritas lain yang juga mewajibkan bank untuk menyampaikan notifikasi awal dan/atau laporan insiden TI, khususnya insiden siber, maka bank menyampaikannya kepada OJK dan otoritas lain tersebut.

Dalam hal jangka waktu yang diberikan oleh otoritas lain lebih singkat daripada jangka waktu yang diberikan OJK maka bank wajib menyampaikan notifikasi awal dan/atau insiden siber kepada OJK pada saat yang bersamaan dengan waktu penyampaian kepada otoritas lain dimaksud.

15. Apa saja muatan tambahan pada laporan kondisi terkini penyelenggaraan TI dalam POJK ini yang belum diatur dalam POJK sebelumnya?

Dengan diterbitkannya POJK ini, terdapat penambahan atas muatan dalam laporan kondisi terkini penyelenggaraan TI yang sebelumnya dikenal sebagai laporan kondisi terkini penggunaan TI, antara lain:

a. hasil penilaian sendiri atas tingkat maturitas keamanan siber;
b. hasil pengujian keamanan siber berdasarkan analisis kerentanan; dan
c. hasil penilaian sendiri atas tingkat maturitas digital bank.

16. Kapan penilaian sendiri atas tingkat maturitas keamanan siber dan tingkat maturitas digital bank mulai dilakukan?

Penilaian sendiri atas tingkat maturitas keamanan siber dan tingkat maturitas digital bank dilaksanakan untuk pertama kali setelah ditetapkan oleh OJK melalui penerbitan Surat Edaran OJK yang mengatur lebih lanjut terkait dengan hal tersebut.

17. **Bagaimana pengaturan mengenai penyampaian laporan hasil audit intern TI dalam POJK ini?**

    Terdapat penyesuaian pengaturan mengenai jangka waktu penyampaian hasil audit intern TI. Dalam POJK ini, hasil audit intern TI disampaikan kepada OJK sebagai bagian dari laporan pelaksanaan dan pokok-pokok hasil audit intern secara semesteran sesuai dengan POJK mengenai penerapan fungsi audit intern bagi bank umum.

18. **Dalam POJK ini tidak lagi terdapat pengaturan mengenai Layanan Perbankan Elektronik, apakah bank tetap dapat menyelenggarakan layanan dimaksud?**

    POJK ini tidak lagi mengatur mengenai penyelenggaraan layanan perbankan elektronik mengingat hal tersebut merupakan produk bank. Meskipun demikian, penyelenggaraan layanan perbankan elektronik telah diatur dalam POJK mengenai penyelenggaraan layanan perbankan digital oleh bank umum. Oleh karena itu, bank tetap dapat menyelenggarakan layanan perbankan elektronik dengan mengacu pada POJK tersebut. Sementara itu, untuk proses perizinan layanan perbankan elektronik, bank mengacu pada POJK mengenai penyelenggaraan produk bank umum.

19. **Apakah OJK mewajibkan bank untuk menggunakan standar tertentu dalam penyelenggaraan TI?**

    Sesuai dengan POJK ini, bank wajib menetapkan standar sebagai acuan dalam penyelenggaraan TI. Namun demikian, OJK tidak mewajibkan bank untuk menggunakan standar tertentu. Bank dapat menggunakan standar yang berlaku sesuai dengan kebutuhan dan kompleksitas bank. Penggunaan atas standar tertentu dapat dikomunikasikan dengan pengawas bank masing-masing.

-ooo-

POJK NO. 11/POJK.03/2022

TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

Jakarta, 2022

Departemen Penelitian dan Pengaturan Perbankan
Otoritas Jasa Keuangan

Executive Summary

- Kebutuhan & Harapan Industri Perbankan serta risiko TI dalam rangka Transformasi Digital (Era Bank 4.0)
- Perkembangan Industri Keuangan Baru dan Ekosistem Keuangan Digital
- Arah Kebijakan Perbankan (RP2I 2020-2025)
- Cetak Biru Transformasi Digital Perbankan

Amandemen

POJK tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (POJK MRTI)

Tujuan Amandemen

Mendukung **Transformasi Digital** dan **Resiliensi Siber** Industri Perbankan

Permasalahan	Analisis	Solusi
Peningkatan akses & konektivitas dalam penggunaan TI berpotensi meningkatkan risiko siber perbankan.	Belum terdapat regulasi mengenai resiliensi siber sektor perbankan.	Penguatan regulasi terkait **keamanan siber (*cybersecurity*)**
Peningkatan kebutuhan pemanfaatan TI menuntut bank untuk menyelenggarakan TI yang andal, aman, efektif, dan efisien.	Pengaturan eksisting hanya berfokus pada aspek manajemen risiko.	Perluasan & penguatan pengaturan terkait aspek **TI, data, manajemen risiko, kolaborasi, & tatanan institusi.**
Adanya kebutuhan penilaian tingkat kematangan bank dalam menyelenggarakan TI secara keseluruhan dalam menghadapi era digitalisasi.	Belum terdapat metode penilaian tingkat kematangan bank dalam menyelenggarakan TI.	Pengaturan metode *assessment* TI bank melalui penilaian ***Digital Maturity Assessment for Bank*** **(DMAB)**

Struktur POJK

BAB I Ketentuan Umum

BAB II Tata Kelola TI Bank

BAB III Arsitektur TI Bank

BAB IV Penerapan Manajemen Risiko Penyelenggaraan TI Bank

BAB V Ketahanan dan Keamanan Siber Bank

BAB VI Penggunaan Pihak Penyedia Jasa TI dalam Penyelenggaraan TI Bank

BAB VII Penempatan Sistem Elektronik dan Pemrosesan Transaksi Berbasis TI

BAB VIII Pengelolaan Data dan Pelindungan Data Pribadi dalam Penyelenggaraan TI Bank

BAB IX Penyediaan Jasa TI oleh Bank

BAB X Pengendalian dan Audit Intern dalam Penyelenggaraan TI Bank

BAB XI Pelaporan

BAB XII Penilaian Tingkat Maturitas Digital Bank

BAB XIII Ketentuan Peralihan

BAB XIV Ketentuan Penutup

Tata Kelola TI Bank

Bank **wajib menerapkan tata kelola TI yang baik** dalam penyelenggaraan TI.

Faktor yang perlu dipertimbangkan oleh Bank dalam penerapan Tata Kelola TI:

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.

Kegiatan yang harus Bank lakukan dalam penerapan Tata Kelola TI:

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.

Tata Kelola TI Bank

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.

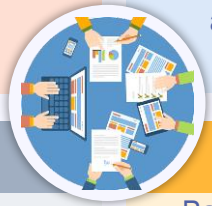
Direksi

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.

Satuan Kerja Penyelenggara TI

- Bank wajib memiliki satuan kerja penyelenggara TI yang bertanggung jawab atas pengelolaan TI.
- Pengelolaan TI paling sedikit berupa aktivitas:
  a. perencanaan;
  b. penyusunan atau pengembangan;
  c. pengoperasian; dan
  d. pemantauan,

  atas kegiatan penyelenggaraan TI.



Dewan Komisaris

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

Komite Pengarah TI

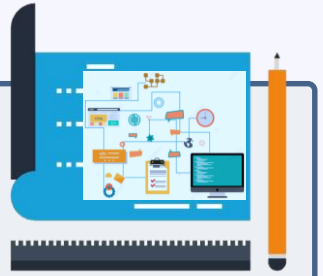
- Bank wajib memiliki komite pengarah TI.
- Komite pengarah TI bertanggung jawab memberikan rekomendasi kepada Direksi terkait dengan penyelenggaraan TI Bank.

Arsitektur TI Bank

Bank wajib memiliki **arsitektur TI.**

Arsitektur TI **disusun secara komprehensif** meliputi **proses:**

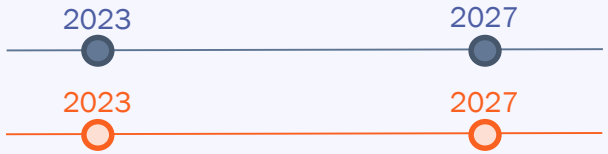
perencanaan → desain → implementasi → kontrol



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

RSTI disusun dalam **jangka panjang** sesuai periode rencana korporasi Bank

Contoh:



Perubahan RSTI dilakukan apabila terdapat kondisi yang secara signifikan memengaruhi sasaran dan strategi TI dalam RSTI

- RSTI disampaikan **maks. akhir bulan November** tahun sebelum periode awal RSTI dimulai
- Perubahan RSTI disampaikan sewaktu-waktu dalam periode RSTI.

Contoh:

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

Manajemen Risiko dalam Penyelenggaraan TI

Bank wajib **menerapkan manajemen risiko secara efektif** dalam penyelenggaraan TI.

Cakupan penerapan manajemen risiko dilaksanakan sesuai dengan:
1. POJK No.18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum; atau
2. POJK No.65/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum Syariah dan Unit Usaha Syariah.

Dalam menerapkan manajemen risiko, Bank melakukan **proses paling sedikit:**

Identifikasi Risiko → Pengukuran Risiko → Pemantauan Risiko → Pegendalian Risiko

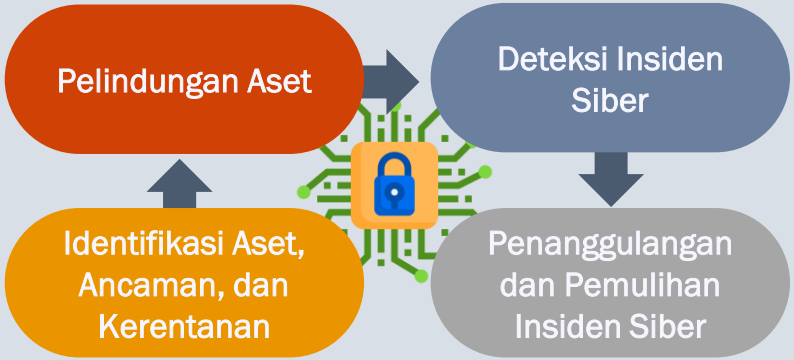
Bank wajib **memiliki Rencana Pemulihan Bencana (*disaster recovery plan*/DRP)** dan **memastikan** bahwa DRP **dapat dilaksanakan**, sehingga **kelangsungan operasional Bank tetap berjalan** saat terjadi bencana dan/atau gangguan pada sarana TI yang digunakan Bank.

a. Uji coba atas DRP*); dan
b. Kaji ulang DRP,
wajib dilakukan paling sedikit **1 (satu) kali dalam 1 (satu) tahun.**

*) untuk seluruh aplikasi dan infrastruktur yang kritikal sesuai hasil analisis dampak bisnis,

Ketahanan dan Keamanan Siber

Bank wajib **menjaga ketahanan siber**, dengan melakukan **proses paling sedikit:**



Dukungan Sistem Informasi Ketahanan Siber

Bank wajib melakukan **penilaian sendiri atas tingkat maturitas keamanan siber.**

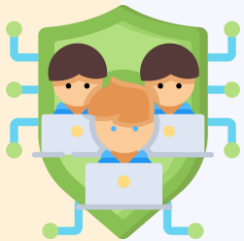
- Secara **tahunan** untuk posisi **akhir bulan Desember.**
- Penyampaian hasil penilaian sebagai bagian dari laporan **kondisi terkini penyelenggaraan TI** Bank.

Bank wajib melakukan **pengujian keamanan siber** berdasarkan:

Analisis Kerentanan	Skenario
- secara berkala **sesuai kebutuhan.** - hasil pengujian sebagai bagian dari **laporan kondisi terkini penyelenggaraan TI** Bank. - contoh: *penetration test.*	- paling sedikit **1 (satu) kali dalam 1 (satu) tahun.** - hasil pengujian disampaikan paling lama **10 (sepuluh) hari kerja** setelah pengujian selesai. - contoh: *cyber incident response* dan *table-top exercise.*

Bank wajib **membentuk unit atau fungsi** yang bertugas **menangani ketahanan dan keamanan siber Bank.**

Unit atau fungsi dimaksud bersifat **independen** terhadap fungsi **pengelolaan TI.**



Penggunaan Pihak Penyedia Jasa TI

Bank dapat **menggunakan pihak penyedia jasa TI** dalam penyelenggaraan TI.

Jika Bank menggunakan pihak penyedia jasa TI maka **Bank wajib memiliki:**

1. kemampuan dalam **melakukan pengawasan** atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa TI.

2. kebijakan dan prosedur dalam penggunaan pihak penyedia jasa TI
   - proses identifikasi kebutuhan penggunaan pihak penyedia jasa TI
   - proses pemilihan pihak penyedia jasa TI
   - tata cara melakukan hubungan kerja sama dengan pihak penyedia jasa TI
   - proses manajemen risiko penggunaan pihak penyedia jasa TI
   - tata cara penilaian kinerja dan kepatuhan pihak penyedia jasa TI

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

Penempatan Sistem Elektronik

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

Bank **dapat** menempatkan Sistem Elektronik pada DC dan/atau DRC di luar wilayah Indonesia sepanjang memperoleh **izin dari Otoritas Jasa Keuangan**. Kriteria Sistem Elektronik dimaksud yaitu Sistem Elektronik yang digunakan untuk:

mendukung analisis terintegrasi

manajemen risiko secara terintegrasi

penerapan APU PPT secara terintegrasi

manajemen intern Bank

pelayanan kepada nasabah secara global, yang memerlukan integrasi.

manajemen komunikasi antara kantor pusat Bank dan kantor cabang

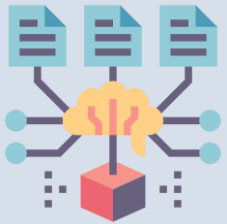
Dalam hal terdapat kondisi yang **mengganggu operasional Bank secara signifikan**, OJK dapat menentukan penempatan Sistem Elektronik pada DC dan/atau DRC di luar wilayah Indonesia selain kriteria tersebut **untuk sementara waktu.**

OJK memberikan izin atau menolak permohonan izin penempatan Sistem Elektronik pada DC dan/atau DRC di luar wilayah Indonesia **paling lama 3 (tiga) bulan** setelah seluruh persyaratan dipenuhi oleh Bank dan dokumen permohonan diterima secara lengkap.

Pengelolaan Data dan Pelindungan Data Pribadi

Bank wajib **mengelola data secara efektif** dalam pemrosesan data Bank untuk mendukung pencapaian tujuan bisnis Bank. Hal tersebut dilakukan dengan memperhatikan:

- Kepemilikan dan Kepengurusan Data
- Kualitas Data
- Sistem Pengelolaan Data
- Sumber Daya Pendukung Pengelolaan Data



Bank wajib melaksanakan **prinsip pelindungan data pribadi** dalam melakukan pemrosesan data pribadi.

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

Dalam hal terdapat kondisi tertentu yang berpotensi meningkatkan risiko bagi pemilik data pribadi, Bank wajib melakukan penilaian dampak atas penerapan prinsip pelindungan data pribadi

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.

Penyediaan Jasa TI oleh Bank

Bank hanya dapat menyediakan jasa TI kepada **lembaga jasa keuangan lain:**

yang diawasi oleh OJK

dan/atau

di luar wilayah Indonesia **yang diawasi** otoritas pengawas dan pengatur lembaga jasa keuangan setempat

dengan terlebih dahulu memperoleh izin OJK untuk setiap rencana penyediaan jasa TI

Bank dapat menyediakan jasa TI **berupa aplikasi** kepada **lembaga jasa keuangan selain bank** sepanjang:

- lembaga jasa keuangan pengguna jasa TI **berada dalam satu grup atau kelompok dengan Bank, dan**
- penggunaan aplikasi ditujukan untuk **mendukung kegiatan operasional yang umum**

Pengendalian Intern dan Audit Intern

Bank **wajib melaksanakan sistem pengendalian intern secara efektif** dalam penyelenggaraan TI, paling sedikit terkait:

- pengawasan & budaya pengendalian
- identifikasi & penilaian risiko
- pengendalian & pemisahan fungsi
- dukungan sistem terkait
- pemantauan & koreksi penyimpangan

Fungsi audit intern TI dilaksanakan secara efektif dan menyeluruh

Memperhatikan POJK mengenai penerapan fungsi audit intern bagi bank umum.

Audit intern TI wajib dilaksanakan paling sedikit 1 kali setahun.

Sesuai dengan kebutuhan, prioritas, & hasil analisis risiko atas penyelenggaraan TI,

Audit Intern TI

Fungsi audit intern TI wajib dikaji ulang paling sedikit 1 kali dalam 3 tahun

Kaji ulang dilakukan oleh pihak ekstern yang independen.

Hasil kaji ulang dan audit TI wajib dilaporkan kepada OJK

- Hasil kaji ulang merupakan bagian dari laporan hasil kaji ulang pihak ekstern yang independen;
- Hasil audit intern TI secara lengkap merupakan bagian dari laporan pelaksanaan & pokok-pokok hasil audit intern

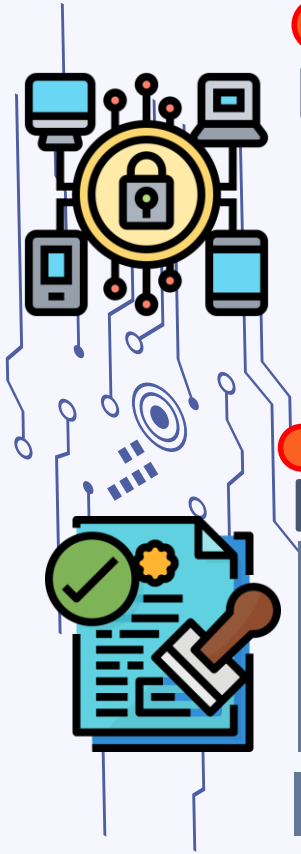
Laporan terkait Penyelenggaraan TI

Laporan Rutin

Nama Laporan	Batas Akhir Penyampaian	Media Penyampaian
Rencana Strategis TI	Akhir November T-1	SIPENA
Rencana Pengembangan TI	Akhir November T-1	APOLO
Kondisi Terkini Penyelenggaraan TI	Hari kerja ke 15 Januari	SIPENA
Hasil kaji ulang atas fungsi audit intern TI	2 bulan setelah periode kaji ulang berakhir	Luring
Hasil audit intern TI	Akhir bulan Juli & akhir bulan Januari	SIPENA

- ✓ Rencana strategis TI dapat dikinikan sewaktu-waktu dengan batas akhir penyampaian setiap akhir bulan November
- ✓ Terdapat tambahan muatan ketentuan dalam laporan kondisi terkini penyelenggaraan TI, yaitu: 1) hasil penilaian sendiri atas tingkat maturitas keamanan siber, 2) hasil pengujian keamanan siber berdasarkan analisis kerentanan, dan 3) hasil penilaian sendiri atas tingkat maturitas digital bank

Laporan non Rutin & Perizinan



Laporan Non Rutin

Nama Laporan	Batas Akhir Penyampaian	Media Penyampaian
Notifikasi awal insiden TI (siber & non siber)	1 x 24 jam setelah insiden diketahui	Sarana elektronik resmi
Laporan tertulis insiden TI (siber & non siber)	5 HK setelah insiden diketahui	SIPENA

Perizinan Penyelenggaraan TI

Nama Laporan	Batas Akhir Penyampaian	Media Penyampaian
Izin penempatan DC/DRC pada SE di luar negeri, pemrosesan transaksi di luar negeri, kegiatan sebagai PJTI	3 bulan sebelum penyelenggaraan, * khusus untuk penempatan DC/DRC & pemrosesan transaksi di luar negeri	SIPENA
Laporan realisasi	3 bulan setelah implementasi	SIPENA

Lainnya

Bank wajib melakukan penilaian sendiri atas **tingkat maturitas digital Bank** secara berkala, paling sedikit 1 kali setahun.

Hasil penilaian wajib dilaporkan sebagai **bagian dari laporan kondisi terkini** penyelenggaraan TI Bank.

Hal-hal yang harus disesuaikan pasca penerbitan POJK ini:

1. Kebijakan, standar, dan prosedur, serta pedoman manajemen risiko penyelenggaraan TI maks. 6 bulan sejak berlakunya POJK ini.
2. Perjanjian kerja sama bagi Bank yang telah menggunakan pihak penyedia jasa TI.
3. Rencana strategis TI sesuai ketentuan dalam POJK ini maks. akhir bulan November 2022.

Bank melaksanakan ketentuan terkait:

- ❑ penilaian sendiri atas tingkat maturitas keamanan siber,
- ❑ pengujian keamanan siber berdasarkan analisis kerentanan,
- ❑ pengujian keamanan siber berdasarkan skenario, dan
- ❑ penilaian sendiri atas tingkat maturitas digital Bank,

untuk pertama kali setelah ditetapkan oleh OJK dalam SEOJK.

POJK ini berlaku 3 bulan sejak diundangkan.

Akses POJK

Available online

sikepo
SISTEM INFORMASI KETENTUAN PERBANKAN ONLINE

https://sikepo.ojk.go.id

ANDROID APP ON Google play

Download on the App Store

TERIMA KASIH

MEDIA BRIEFING – KEPALA EKSEKUTIF PENGAWAS PERBANKAN

TERKAIT PERATURAN OTORITAS JASA KEUANGAN

NOMOR 11/POJK.03/2022 TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

JAKARTA, 4 AGUSTUS 2022

---

1. Transformasi digital di sektor perbankan adalah awal dari suatu masa depan dan menjadi suatu keniscayaan. Tuntutan akselerasi digital di sektor perbankan semakin mengemuka dan sudah menjadi ekspektasi masyarakat dan dunia usaha. Dari sisi ini, kita mencermati bahwa pandemi Covid-19 merupakan *blessing* dan menjadi momentum perubahan pada berbagai aspek kehidupan sosial dan ekonomi masyarakat secara menyeluruh. Pandemi dengan segala pembatasan sosial yang menyertainya menimbulkan tatanan baru *(new normal)* bagi masyarakat dalam melakukan transaksi ekonomi dan pola pembayarannya. Pergeseran perilaku dan orientasi masyarakat dari *physical* ke arah *virtual economy* ini akan bersifat permanen, termasuk tuntutan model layanan perbankan yang berbeda dari sebelumnya.

2. Perkembangan teknologi informasi dan keuangan yang revolusioner ini telah meningkatkan minat masyarakat untuk merasakan *digital experience* dalam setiap interaksinya dengan bank. Mencermati hal ini, menjadi keharusan bagi perbankan untuk melakukan digitalisasi pada semua aspek termasuk aktivitas *core-banking* baik pada fungsi *front-office, middle-office,* dan *back-office* serta mengubah proses transaksi dari *analog channels* menjadi *digital channels.*

3. Lebih lanjut, perubahan lingkungan bisnis yang dinamis sebagai dampak digitalisasi semakin menuntut Bank untuk lebih berorientasi ke arah *customer centric* melalui interaksi yang lebih intens dengan nasabah untuk memahami perilaku ekonominya. Tuntutan inovasi dan kelenturan dalam menyajikan produk dan layanan yang disesuaikan dengan karakteristik dan kebutuhan nasabah menjadi keharusan. Dengan pola ini, nasabah dapat merasakan *digital banking experience* yang *unique* dan *personalized.*

4. Dinamika-dinamika tersebut memberikan efek rembetan pada inovasi konektivitas dan kolaborasi bank dengan *ecosystem* baru yang membentuk ekonomi digital melalui pembentukan digital banking. Oleh karena itu paradigma *closed-banking* yang sebelumnya menjadi dogma perbankan telah berubah pada pola *open ban*king dengan memanfaatkan berbagai infrastruktur pendukung seperti *open API, cloud computing, artificial intelligence, machine learning* dll.

5. Menyikapi perubahan lingkungan bisnis tersebut, perbankan nasional harus siap bertransformasi. Bank yang belum *'move on'* dan masih setia dengan layanan perbankan tradisionalnya, harus bersiap untuk tersisih dan harus rela didera *flight to service* ataupun *flight to digital* akibat ditinggalkan oleh nasabah yang beralih ke bank-bank yang memberikan layanan secara digital.

Akselerasi Transformasi Digital dan Potensi Risiko kedepan

6. Masifnya akselerasi transformasi digital di sektor keuangan khususnya perbankan menimbulkan pertanyaan *"sejauh mana perbankan telah memitigasi potensi risiko baru atau mengenali the unknown-unknown risk?"*

7. Perkembangan digital banking dengan seluruh infrastruktur yang menyertainya tentunya akan memicu tantangan tersendiri dalam tranformasi bank digital kedepan. Di era teknologi dan disrupsi

digital yang perlu diwaspadai adalah ***potensi serangan siber***. Sangat disadari bahwa penggunaan teknologi informasi secara masif akan meningkatkan risiko serangan siber yang juga dapat berakibat pada kebocoran/pencurian data nasabah. Bank juga perlu memperhatikan potensi risiko yang belum pernah terjadi sebelumnya antara lain *security and system failure risk*, *digital black-out*, maupun potensi sistemik akibat *digital bank-run*.

8. Terkait dengan risiko serangan Siber, berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), sektor keuangan dan utamanya perbankan, merupakan sektor yang berisiko tinggi menjadi target serangan siber. Diantara kasus serangan yang dominan antara lain serangan ransomware dan phishing. Oleh karena itu untuk meningkatkan resiliensi sektor perbankan atas berbagai pola baru serangan siber, bank perlu melakukan berbagai upaya untuk menjaga ketahanan dan keamanan siber secara berkelanjutan. Beberapa hal yang dapat dilakukan bank antara lain dengan melakukan pengujian keamanan siber, penilaian sendiri atas tingkat maturitas keamanan siber serta pelaporan insiden siber.

9. **Penggunaan teknologi yang masif juga berimbas pada semakin besarnya penggunaan pihak ketiga *(outsourcing)* yang berpotensi menimbulkan risiko lain pada aktivitas Bank seperti risiko operasional**. Lebih lanjut, kecanggihan teknologi perlu diimbangi oleh kesiapan organisasi antara lain ***digital leader*** dan ***digital talent*** **yang memadai, baik dari sisi kualitas maupun kuantitasnya, budaya organisasi yang berorientasi digital dan desain organisasi yang mendukung transformasi digital**.

10. Dari berbagai observasi tersebut, aturan terkait penyelenggaraan tehnologi informasi menjadi sangat relevan. Tidak hanya dari sisi perbankan, regulator pun menghadapi tantangan dimana peraturan yang ada saat ini belum sepenuhnya mengakomodasi perkembangan industri. Oleh karena itu, **dukungan *regulatory framework*** yang suportif akan terus didorong sehingga bank mampu bergerak lebih cepat dalam menawarkan produk dan layanan digital perbankan dengan tetap memperhatikan aspek kehati-hatian.

Respon Kebijakan

11. ***Lantas apa saja yang disiapkan OJK sebagai regulator dari sisi kebijakan?*** Untuk merespon tren perkembangan industri perbankan yang mengarah pada digitalisasi yang masif tersebut, termasuk dinamika selama pandemi, serta perubahan landscape yang menyertainya, OJK telah menerbitkan Cetak Biru Transformasi Digital Perbankan pada tahun 2021. Penerbitan *Blueprint* yang merupakan panduan akselerasi transformasi digital ini dilandasi semangat dan tujuan agar industri perbankan Indonesia secara kelembagaan dapat mencapai skala ekonomi yang lebih tinggi, lebih efisien, lebih berdaya saing, adaptif terhadap perubahan ekspektasi masyarakat serta kontributif bagi perekonomian.

12. Sebagai tindak lanjut dari diterbitkannya Cetak Biru Transformasi Digital Perbankan, OJK menerbitkan Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum (POJK PTI) yang mengadopsi konsep *principle* dari *blueprint* yang penting untuk dituangkan menjadi *'rule'*.

13. Pengaturan POJK PTI ini telah mengakomodasi seluruh pilar dalam cetak biru transformasi digital perbankan. Diawali dengan pengaturan terkait tata kelola penyelenggaraan TI yang bertujuan untuk meningkatkan peran direksi, dewan komisaris dan seluruh pihak yang berkaitan dengan

penyelenggaraan TI di bank. Dengan demikian bank dapat memaksimalkan *value added* dari penyelenggaraan TI sesuai dengan strategi digitalisasi perbankan yang diikuti dengan mitigasi risiko yang memadai.

14. Selanjutnya dalam mendukung tata kelola TI, bank perlu memastikan bahwa penyelenggaraan TI dapat memenuhi kebutuhan organisasi. Hal tersebut dilakukan dengan penyusunan arsitektur TI yang menerjemahkan strategi organisasi menjadi rencana sistem informasi berdasarkan pemahaman atas strategi organisasi. Arsitektur TI merupakan cetak biru yang menjadi landasan bagi bank dalam mengatur, merencanakan dan menentukan TI yang mendukung proses bisnis organisasi.

Jakarta, 4 Agustus 2022

Kepala Eksekutif Pengawas Perbankan

Dian Ediana Rae

=== o0o ===