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-