RINGKASAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR 29/SEOJK.03/2022

TENTANG KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

1. Latar Belakang

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (POJK PTI), perlu untuk mengatur ketentuan pelaksanaan lebih lanjut dalam Surat Edaran Otoritas Jasa Keuangan. Salah satu ketentuan lebih lanjut dari POJK PTI adalah SEOJK tentang ketahanan dan keamanan siber bagi bank umum.

2. Pokok Pengaturan

SEOJK tentang Ketahanan dan Keamanan Siber bagi Bank Umum ini terdiri dari 10 Bab, dengan substansi pengaturan sebagai berikut:

A. BAB I – KETENTUAN UMUM

Bab ini berisi mengenai *spirit* pengaturan dari SEOJK. Selain itu terdapat pengertian dari ketahanan siber, keamanan siber, laporan insiden siber, dan notifikasi awal insiden siber, yang akan dibahas lebih lanjut dalam beberapa bab selanjutnya.

B. BAB II – PENILAIAN RISIKO INHEREN TERKAIT KEAMANAN SIBER Bab ini antara lain mengatur:

1) penilaian risiko inheren terkait keamanan siber oleh Bank, dengan memperhatikan paling sedikit 4 (empat) faktor penilaian yaitu teknologi, produk bank, karakteristik organisasi, dan rekam jejak insiden siber;
2) penilaian risiko inheren terkait keamanan siber, yang dilaksanakan secara tahunan untuk posisi akhir bulan Desember. Hasil penilaian risiko inheren terkait keamanan siber disampaikan kepada OJK sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank; dan
3) tingkat risiko inheren terkait keamanan siber dipertimbangkan sebagai parameter atau indikator tambahan dari tingkat risiko inheren untuk aspek TI pada risiko operasional dalam penilaian tingkat kesehatan Bank.

C. BAB III – PENERAPAN MANAJEMEN RISIKO TERKAIT KEAMANAN SIBER Bab ini mengatur mengenai:

1) penerapan manajemen risiko terkait keamanan siber oleh Bank, yang mencakup 4 (empat) aspek, yaitu:
   a) tata kelola risiko terkait keamanan siber;

b) kerangka manajemen risiko terkait keamanan siber;
c) proses manajemen risiko, kecukupan sumber daya manusia, serta kecukupan sistem informasi manajemen risiko, terkait keamanan siber; dan
d) sistem pengendalian risiko terkait keamanan siber;

2) penerapan manajemen risiko terkait keamanan siber disesuaikan dengan karakteristik dan kompleksitas bisnis Bank.

D. BAB IV – PENERAPAN PROSES KETAHANAN SIBER BAGI BANK UMUM

Bab ini mengatur mengenai proses yang dilakukan Bank untuk menjaga ketahanan siber, yaitu:

1) identifikasi aset, ancaman, dan kerentanan;
2) pelindungan aset;
3) deteksi insiden siber; dan
4) penanggulangan dan pemulihan insiden siber.

E. BAB V PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER Bab ini mengatur antara lain mengenai:

1) penilaian tingkat maturitas keamanan siber oleh Bank, yang dilakukan secara tahunan untuk posisi akhir bulan Desember;
2) penilaian tingkat maturitas keamanan siber, yang mencakup penilaian terhadap:
   a) kualitas penerapan manajemen risiko terkait keamanan siber; dan
   b) kualitas penerapan proses ketahanan siber;
3) penilaian tingkat maturitas keamanan siber, yang dilaksanakan secara tahunan untuk posisi akhir bulan Desember. Hasil penilaian tingkat maturitas keamanan siber disampaikan kepada OJK sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank; dan
4) tingkat maturitas keamanan siber dipertimbangkan sebagai parameter atau indikator tambahan dari kualitas penerapan manajemen risiko untuk aspek TI pada risiko operasional dalam penilaian tingkat kesehatan Bank.

F. BAB VI – TINGKAT RISIKO TERKAIT KEAMANAN SIBER

Bab ini mengatur mengenai tingkat risiko terkait keamanan siber, yang ditetapkan berdasarkan penilaian risiko inheren terkait keamanan siber dan tingkat maturitas keamanan siber.

Penetapan tingkat risiko terkait keamanan siber dilakukan secara tahunan untuk posisi akhir bulan Desember. Tingkat risiko terkait keamanan siber disampaikan kepada OJK sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.

G. BAB VII – PENGUJIAN KEAMANAN SIBER

Bab ini mengatur mengenai jenis dan pelaporan hasil pengujian keamanan siber yang dilakukan oleh Bank.

1) Pengujian Keamanan Siber Berdasarkan Analisis Kerentanan
   a) Bertujuan untuk melihat titik lemah dari sistem Bank;
   b) Dilaksanakan secara berkala berdasarkan evaluasi intern Bank, yang diawali dengan pelaksanaan identifikasi kerentanan yang kemudian dilanjutkan dengan *penetration test;*
   c) Hasil pengujian disampaikan kepada OJK sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.
2) Pengujian Keamanan Siber Berdasarkan Skenario
   a) Bertujuan untuk memvalidasi proses penanggulangan dan pemulihan insiden siber pada Bank;
   b) Dilaksanakan secara berkala, paling sedikit 1 (satu) kali dalam 1 (satu) tahun;
   c) Hal yang perlu diperhatikan dalam pengujian keamanan siber berdasarkan skenario, seperti pengujian dalam bentuk simulasi serangan harus dilakukan secara terkendali di bawah pengawasan ketat;
   d) Hasil pengujian disampaikan kepada OJK paling lama 10 (sepuluh) hari kerja setelah pengujian keamanan siber selesai dilaksanakan.
3) Bank dapat melakukan pengujian keamanan siber secara mandiri atau menggunakan pihak ketiga dengan tetap memperhatikan hal-hal tertentu.

H. BAB VIII – UNIT ATAU FUNGSI YANG MENANGANI KETAHANAN DAN KEAMANAN SIBER

Bab ini antara lain mengatur mengenai:

1) Tugas dari unit atau fungsi yang menangani ketahanan dan keamanan siber Bank, yaitu mengoordinasikan dan/atau melaksanakan:
   a) proses ketahanan siber Bank;
   b) penilaian sendiri atas risiko inheren terkait keamanan siber dan tingkat maturitas keamanan siber;
   c) penetapan tingkat risiko terkait keamanan siber; dan
   d) pengujian keamanan siber;
2) Unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber bersifat independen terhadap fungsi pengelola TI;

3) Unit atau fungsi yang menangani ketahanan dan keamanan siber mengoordinasikan tim tanggap insiden siber, termasuk inisasi pembentukannya.

4) Unit atau fungsi yang menangani ketahanan dan keamanan siber memastikan bahwa tim tanggap insiden siber:
   a) memiliki kapasitas dan kemampuan terkait penanganan insiden siber;
   b) dapat bekerja sama dengan unit atau fungsi terkait;
   c) memiliki sumber daya analisis insiden;
   d) dapat bekerja sama secara efektif dengan fungsi intelijen ancaman siber;
   e) dipimpin oleh pejabat yang berasal dari unit atau fungsi yang menangani ketahanan dan keamanan siber; dan
   f) memiliki narahubung untuk mendukung koordinasi dalam pelaksanaan tugas.

I. BAB IX – LAPORAN INSIDEN SIBER

Bab ini mengatur mengenai insiden siber serta mekanisme pelaporan insiden siber.

1) Insiden siber merupakan ancaman siber berupa upaya, kegiatan, dan/atau tindakan yang mengakibatkan Sistem Elektronik tidak berfungsi sebagaimana mestinya.
2) Bank perlu melakukan pemantauan atas insiden siber sebagai bentuk komunikasi kepada para pemangku kepentingan dan pengendalian atas pengelolaan ketahanan dan keamanan siber.
3) Pelaporan Insiden Siber
   a) notifikasi awal insiden siber
      (1) berisi informasi awal yang tersedia terkait insiden siber;
      (2) disampaikan kepada OJK melalui sarana elektronik secara tertulis paling lama 24 (dua puluh empat) jam setelah insiden siber diketahui oleh Bank;
      (3) ditujukan kepada pengawas Bank yang bersangkutan;
   b) laporan insiden siber
      (1) berisi informasi terkait insiden siber yang lebih lengkap;
      (2) disampaikan secara daring melalui sistem pelaporan OJK paling lama 5 (lima) hari kerja setelah insiden siber diketahui.
4) Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal dan/atau laporan insiden siber dengan jangka waktu

yang lebih cepat, Bank menyampaikan notifikasi awal dan/atau laporan insiden siber kepada OJK pada saat yang bersamaan sesuai dengan pengaturan otoritas lain dimaksud.

J. BAB X KETENTUAN PENUTUP

Bab ini mengatur mengenai keberlakuan dari SEOJK, yaitu pada tanggal ditetapkan.