KPMG Cyber Newsflash

Ketahanan dan keamanan siber bagi sektor perbankan Indonesia

Peningkatan akses & konektivitas dalam penggunaan teknologi informasi (TI) berpotensi meningkatkan risiko siber perbankan. Maka dari itu, perlu adanya regulasi mengenai ketahanan siber pada sektor perbankan. Untuk mendukung transformasi digital dan ketahanan siber industri perbankan, Otoritas Jasa Keuangan (OJK) menerbitkan Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (POJK 11 - PTI). POJK 11 – PTI menggantikan Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum (POJK 38 - MRTI).

Pada 27 Desember 2022, Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 (SEOJK 29) tentang Ketahanan dan Keamanan Siber Bagi bank Umum diterbitkan untuk mendetailkan area terkait keamanan siber yang disebutkan pada POJK 11 (POJK 11 - PTI). SEOJK 29 ini terdiri dari 10 bab, dengan ikhtisar sebagai berikut:

- **Bab I – Ketentuan umum**
  Penjelasan definsi ketahanan siber, keamanan siber, laporan insiden siber, dan notifikasi awal insiden siber.

- **Bab II – Penilaian risiko inheren terkait keamanan siber**
  Risiko inheren keamanan siber berfokus pada beberapa parameter seperti teknologi, produk bank, karakteristik organisasi, dan rekam jejak insiden siber. Tingkat penilaian risiko inheren terbagi menjadi 5 kategori: *1-Low*, 2-*Low to moderate*, 3-*Moderate*, *4-Moderate to high*, dan 5-*High*.

- **Bab III – Penerapan manajemen risiko terkait keamanan siber**
  Penerapan manajemen risiko keamanan siber berfokus pada beberapa parameter seperti tata kelola, kerangka kerja manajemen risiko keamanan siber, proses manajemen risiko keamanan siber dan sistem pengendalian risiko.

- **Bab IV – Penerapan proses ketahanan siber bagi bank umum**
  Proses ketahanan siber paling sedikit meliputi identifikasi aset, ancaman dan kerentanan, perlindungan aset, deteksi insiden siber, penanggulangan dan pemulihan insiden siber.

- **Bab V – Penilaian tingkat maturitas keamanan siber**
  Berdasarkan penilaian kualitas penerapan manajemen risiko untuk proses keamanan siber dan ketahanan siber. Penetapan kualitas penerapan manajemen risiko terkait keamanan siber dibagi menjadi 5 kategori: 1-*Strong*, 2-*Satisfactory*, 3-*Fair*, 4-*Marginal*, dan 5-*Unsatisfactory*. Selain itu, terdapat 5 tingkat maturitas keamanan siber yaitu Tingkat 1-5.

- **Bab VI – Tingkat risiko terkait keamanan siber**
  Tingkat risiko keamanan siber ditentukan berdasarkan penilaian tingkat risiko inheren keamanan siber dan tingkat maturitas keamanan siber.

- **Bab VII – Pengujian keamanan siber**
  Terdiri dari 2 jenis, yaitu berdasarkan analisis kerentanan dan skenario. Bank dapat melakukan pengujian keamanan siber secara mandiri atau menggunakan pihak ketiga.

- **Bab VIII – Unit atau fungsi yang menangani ketahanan dan keamanan siber bank**
  Bank harus membentuk unit/fungsi khusus yang independen terhadap operasional TI. Unit/fungsi khusus ini bertanggung jawab untuk menangani keamanan dan ketahanan siber termasuk koordinasi tim tanggap insiden keamanan siber. Lebih lanjut, unti/fungsi khusus ini menjalankan **proses ketahanan siber bank, penilaian sendiri atas risiko inheren dan tingkat maturitas keamanan siber, penetapan tingkat risiko keamanan siber, dan pengujian keamanan siber.**

  Tim dari unit/fungsi khusus ini harus dipastikan memiliki
  - Kompetensi, kapasitas dan kapabilitas.
  - Koordinasi dan kolaborasi.
  - Sumber daya dan akses.
  - Kepemimpinan.

- **Bab IX – Laporan insiden siber**
  Insiden siber merupakan kejadian kritis, penyalahgunaan, dan/atau aktivitas kejahatan dalam penyelenggaraan sistem elektronik. Pemantauan insiden siber harus dilakukan untuk menjaga ketahanan dan keamanan siber. Insiden siber harus dilaporkan kepada OJK.

- **Bab X – Penutup**
  Ketentuan dalam SEOJK 29 ini mulai berlaku pada tanggal 27 Desember 2022.

Laporan terkait keamanan siber

Laporan insiden siber	Tingkat risiko inheren keamanan siber	Tingkat maturitas keamanan siber	Tingkat risiko keamanan siber	Hasil pengujian keamanan siber
• Notifikasi awal insiden siber: paling lama **1x24** jam, melalui sarana elektronik secara tertulis (seperti email). • Laporan insiden siber: paling lama **5 hari kerja**, mencakup: – **Informasi pelapor dan informasi umum.** – **Penilaian dampak** – **Kronologi kejadian** – ***Root cause analysis.*** – **Penilaian akhir.**	• **Tahunan**: periode akhir **Desember**. • Disampaikan kepada OJK: paling lambat **15 hari kerja setelah** pelaporan akhir tahun. • Pelaporan pertama **FY22**: disampaikan kepada OJK paling lambat akhir **Juni 2023.** • Dipertimbangkan sebagai parameter atau indikator tambahan dari tingkat **risiko inheren aspek TI pada risiko operasional**	• **Tahunan**: periode akhir **Desember**. • Disampaikan kepada OJK: paling lambat **15 hari kerja setelah** pelaporan akhir tahun. • Pelaporan pertama **FY22**: disampaikan kepada OJK paling lambat akhir **Juni 2023.** • Termasuk **penilaian kualitas:** – **Penerapan manajemen risiko untuk keamanan siber; dan** – **Penerapan proses ketahanan siber.**	• Berdasarkan **penilaian risiko inheren keamanan siber dan tingkat maturitas keamanan siber.** • **Maksimum setinggi** tingkat risiko inheren keamanan siber. • Dapat diperhitungkan **sebagai bagian dari penilaian tingkat kesehatan bank.**	• **Analisis kerentanan** (seperti penetration testing). Disampaikan kepada OJK: paling lambat **15 hari kerja setelah** pelaporan akhir tahun. • **Skenario** (seperti *table-top exercise, cyber range exercise, social engineering exercise, adversarial attack simulation exercise,* dan/atau metode pengujian lainnya). Hasil pengujian disampaikan kepada OJK paling lambat **10 hari kerja setelah** pengujian dilakukan. • **Pengujian keamanan siber pertama kali dilakukan oleh Bank pada tahun 2023.**

Prespektif SEOJK dari *three lines model*

Governing body	*First line*	*Second line*	*Third line*
Governing body bertanggungjawab kepada pemangku kepentingan untuk memantau organisasi. Terdapat 22 klausul dan 36 kontrol dalam SEOJK terkait tanggung jawab *governing body* seperti: • Pengawasan aktif dan tanggung jawab penuh • Ketersediaan dan kecukupan sumber daya • Budaya dan kesadaran • Formalisasi, implementasi, komunikasi, pembaharuan strategi, kerangka kerja, kebijakan, prosedur, limit risiko • Evaluasi, pengawasan, dan pengkajian berkala • Mengarahkan implementasi dan tindakan perbaikan • Penugasan peran dan tanggung jawab	*First line* merupakan pemiik bisnis yang bertanggung jawab langsung terhadap proses bisnis dan mematuhi kebijakan serta prosedur. Terdapat 32 klausul dan 50 kontrol yang terkait dengan tanggung jawab dari first line. *First line – Cyber/IT security:* • Implementasi kontrol internal dan proses ketahanan siber *(cyber resilience)* • Penilaian dan pelaporan tingkat maturitas keamanan siber • Pengujian keamanan siber secara berkala • Pemantauan risiko dan pelaporannya	*Second line* merupakan fungsi khusus untuk membantu memantau dan merancang aturan dan stategi untuk dipatuhi oleh *first line*. Terdapat 21 klausul dan 35 kontrol yang berkaitan dengan tanggung jawab *second line*. Model *line* ini umumnya mengacu kepada fungsi manajemen risiko. *Second line – Cyber risk management*: • Kebijakan dan strategi manajemen risiko keamanan siber • Pemantauan: kebijakan vs implementasi • Penilaian ketahanan siber • Meninjau dampak paparan risiko. • Proses manajemen risiko siber. • Peninjauan dan evaluasi berkala atas penerapan manajemen risiko keamanan siber.	*Third line* merupakan pihak independen yang memastikan kegiatan manajemen risiko telah dilakukan sesuai dengan ketentuan dan peraturan yang berlaku. Terdapat 11 klausul dan 22 kontrol yang terkait dengan tanggung jawab *third line*. Model *line* ini umumnya mengacu pada fungsi audit internal. *Third line – Internal audit:* • Peninjauan dan evaluasi berkala atas manajemen risiko keamanan siber. • Pemantauan remediasi dan tindak lanjut. • Pelaporan perbaikan dan temuan audit yang belum diselesaikan kepada dewan komisaris dan/atau direksi.

SEOJK 29 merupakan regulasi pertama tentang keamanan siber di sektor perbankan yang secara spesifik membahas tentang penerapan kendali internal keamanan siber yang mumpuni di bank, baik bank umum konvensional maupun bank syariah. Dengan metode penilaian sendiri, bank perlu mulai untuk menerapkan implementasi kendali keamanan siber berdasarkan pendekatan berbasis risiko. Mempertimbangkan hal tersebut, SEOJK 29 ini relevan dengan sektor perbankan Indonesia, mengingat bahwa setiap bank memiliki kondisi yang unik, maka risiko keamanan siber yang dihadapi akan berbeda satu sama lainnya, sehingga kendali keamanan siber untuk setiap bank perlu disesuikan.

Contact us

KPMG Siddharta Advisory
35th Floor, Wisma GKBI
28, Jl. Jend. Sudirman
Jakarta 10210, Indonesia
T: +62 (0) 21 574 0877
F: +62 (0) 21 574 0313

Irwan Djaja
Head of Advisory Services
Irwan.Djaja@kpmg.co.id

Freddie Mulyadi
Partner, IT Assurance & Cyber Security
Freddie.Mulyadi@kpmg.co.id

Eric Junatra
Senior Manager, Cyber Security
Eric.Junatra@kpmg.co.id

home.kpmg/id

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.