KEBIJAKAN TEKNOLOGI INFORMASI
PT BANK SYARIAH INDONESIA, TBK

Pendahuluan

Unit Kerja Teknologi Informasi merupakan bagian penting yang secara langsung menunjang kelancaran operasional serta pelayanan bank kepada masyarakat. Seiring pesatnya perkembangan teknologi perbankan, muncul pula tantangan baru, khususnya meningkatkan risiko, termasuk risiko keamanan siber. Karena itu, bank dituntut untuk meningkatkan tingkat kematangan dalam penyelenggaraan teknologi informasi melalui penerapan tata kelola yang baik dan terukur. Dengan tata kelola yang tepat, penyelenggaraan TI tidak hanya berfungsi sebagai penunjang operasional, tetapi juga mampu memberikan nilai tambah yang signifikan dalam mendukung pencapaian tujuan bisnis serta berkontribusi pada pencapaian visi dan misi bank.

Untuk itu, diperlukan sebuah pedoman komprehensif berupa Kebijakan Teknologi Informasi Bank. Pedoman ini berfungsi menyamakan pemahaman seluruh jajaran mengenai arah dan prinsip penyelenggaraan TI, sekaligus memberikan acuan bagi unit kerja dalam melaksanakan aktivitas terkait perencanaan, pengembangan, pengelolaan, pengamanan, serta monitoring sistem. Dengan adanya kebijakan ini, diharapkan seluruh potensi risiko dapat dimitigasi, dikelola, dan dikendalikan dengan baik, sehingga TI benar-benar menjadi penopang utama tercapainya tujuan bisnis dan keberlangsungan bank.

Dasar Penyusunan

1. Peraturan Bank Indonesia (PBI) Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran berikut perubahannya.
2. Peraturan Otoritas Jasa Keuangan No. 11/POJK.03/2022 tanggal 06 Juli 2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum
3. Peraturan Bank Indonesia No. 2 Tahun 2024 tanggal 18 April 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain Yang Diatur dan Diawasi Bank Indonesia.
4. Surat Edaran Otoritas Jasa Keuangan No.29/SEOJK.03/2022 tanggal 27 Desember 2022 perihal Ketahanan dan Keamanan Siber Bagi Bank Umum.

Referensi

Kebijakan Teknologi Informasi PT Bank Syariah Indonesia, Tbk. Tanggal 22 Juli 2024.

Wewenang dan Tanggung Jawab

Penyelenggaraan Teknologi Informasi Bank harus didasarkan pada tata kelola yang baik, dengan pembagian wewenang dan tanggung jawab yang jelas bagi Direksi, Dewan Komisaris, serta pejabat terkait di setiap jenjang.

1. Dewan Komisaris: bertugas mengevaluasi, mengarahkan, dan memantau strategi serta tata kelola TI, termasuk kebijakan manajemen risiko, perencanaan dan pelaksanaan audit, serta pengelolaan keamanan TI guna menjamin ketersediaan, kerahasiaan, dan keakuratan informasi.
2. Direksi: bertugas mengatur strategi dan kebijakan TI, memantau tata kelola serta manajemen risiko, memastikan ketersediaan sumber daya dan peningkatan kompetensi SDM, serta menjamin kontrak dengan pihak ketiga melindungi kepentingan bank.
3. Komite Pengarah Teknologi Informasi: bertanggung jawab memberikan rekomendasi kepada Direksi terkait strategi dan kebijakan TI, memastikan kesesuaian proyek dengan rencana Bank, memantau kinerja dan risiko investasi TI, serta mendukung penyelesaian masalah dan kecukupan sumber daya agar TI efektif menunjang bisnis Bank.
4. Satuan kerja penyelenggara TI: bertanggung jawab atas pengelolaan TI yang terdiri atas perencanaan, penyusunan atau pengembangan, pengoperasian, dan pemantauan.

Ketentuan Umum Penerapan Tata Kelola TI Bank

1. Bank wajib mempertimbangkan strategi bisnis, ukuran, kompleksitas, peran TI, metode pengadaan, risiko, standar, dan aturan hukum.
2. Bank melakukan evaluasi, pengarahan, pemantauan strategi TI, serta penyelarasan dan pengorganisasian unit terkait.
3. Bank mendefinisikan, mengakuisisi, dan mengimplementasikan solusi TI serta menyediakan dukungan operasional.
4. Bank memantau kinerja TI agar sesuai target, pengendalian internal, dan peraturan.
5. Tata kelola TI berlaku untuk seluruh unit pengelola dan pengguna TI.
6. Bank wajib memetakan proses bisnis, struktur organisasi, kebijakan, alur informasi, SDM, budaya TI, infrastruktur, dan aplikasi.
7. Bank harus memastikan sinergi di seluruh aspek tata kelola TI.
8. Kebijakan, standar, dan prosedur tata kelola TI diterapkan konsisten dan berkesinambungan.
9. Kebijakan dan prosedur harus dikaji ulang dan diperbarui secara berkala.
10. Wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan pejabat terkait harus jelas.

Penerapan Manajemen Risiko

Pengamanan informasi menjadi aspek penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data serta mendukung kelangsungan operasional Bank. Beberapa kewajiban utama Bank terkait pengamanan informasi adalah sebagai berikut:

a. Memastikan pengamanan informasi dilaksanakan secara efektif dan efisien.
b. Pengamanan mencakup aspek SDM, proses, teknologi, fisik, dan lingkungan TI.
c. Ruang lingkup pengamanan informasi mencakup aset, SDM, teknologi, proses, dan kepatuhan regulasi untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi.
d. Pengamanan dilakukan berdasarkan hasil penilaian risiko atas informasi Bank.
e. Jaringan komunikasi wajib memenuhi prinsip kerahasiaan, integritas, dan ketersediaan.

Ketentuan Umum Dalam Ketahanan Siber Bank

1. Menjaga ketahanan siber dengan melakukan proses paling sedikit:
    a) Mengidentifikasi aset, ancaman, dan kerentanan melalui manajemen dan inventarisasi aset TI, pemantauan serta identifikasi kerentanan dan ancaman siber terkini, serta pengujian keamanan siber secara berkala.
    b) Bank melindungi aset dengan menerapkan kontrol keamanan komprehensif, pemeliharaan dan pembaruan berkala, manajemen keamanan data, jaringan, perangkat, akses, serta kerja sama dengan penyedia TI (termasuk *cloud*), disertai praktik *secure coding* dan untuk menjaga kerahasiaan, integritas, dan ketersediaan sistem.
    c) Bank wajib memiliki proses deteksi insiden siber yang memadai melalui *baseline performance*, pemantauan aktivitas mencurigakan dan kerentanan secara berkelanjutan, serta analisis ancaman untuk memastikan penanganan insiden efektif dan mencegah gangguan layanan.
    d) Bank wajib memiliki rencana penanggulangan dan pemulihan insiden siber yang jelas, dengan tim tanggap khusus, prosedur pemulihan untuk meminimalkan dampak, analisis dan pelaporan insiden, serta evaluasi pasca insiden sebagai bahan perbaikan berkelanjutan.
2. Bank memastikan proses untuk menjaga ketahanan siber didukung dengan sistem informasi ketahanan siber yang memadai.

Penilaian Tingkat Maturitas Keamanan Siber

1. Bank wajib melakukan penilaian sendiri atas tingkat maturitas keamanan siber.
2. Penilaian dilakukan tahunan sesuai periode regulator.
3. Tujuannya untuk mengukur kondisi keamanan, menemukan kelemahan, dan meningkatkan ketahanan Bank.
4. Penilaian bisa diperbarui sewaktu-waktu bila diperlukan.
5. Hasil penilaian wajib disampaikan ke OJK.
6. Bank wajib melakukan pengujian keamanan siber berdasarkan analisis kerentanan dan skenario.
7. Bank wajib membentuk unit/fungsi khusus untuk menangani ketahanan dan keamanan siber.
8. Unit/fungsi keamanan siber harus independen dari pengelolaan TI.

Prinsip Dasar Pelaksaan Ketahanan dan Keamanan Siber (KKS)

1. Kejelasan peran dan tanggung jawab
2. Strategi yang komprehensif
3. Manajemen risiko siber terintegrasi dengan enterprise risk management
4. Integrasi dengan budaya KKS
5. Kesiapan menghadapi insiden siber

Penutup

Kebijakan ini merupakan wujud nyata dari komitmen BSI dalam meningkatkan ketahanan dan keamanan teknologi dan informasi agar BSI memiliki ketahanan siber yang efektif dalam mendeteksi hinggamengatasi ancaman keamanan siber.

Kebijakan ini akan ditinjau dan diperbarui kembali apabila terdapat hal-hal yang belum diatur atau karenanya adanya perubahan peraturan/ketentuan eksternal dan/atau kebijakan internal perusahaan.