Yth.

1. Direksi Bank Umum Konvensional; dan
2. Direksi Bank Umum Syariah,

di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 5/OJK, Tambahan Lembaran Negara Republik Indonesia Nomor 5/OJK) yang selanjutnya disebut sebagai POJK PTI, perlu untuk mengatur ketentuan pelaksanaan mengenai ketahanan dan keamanan siber bagi bank umum dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Pesatnya perkembangan Teknologi Informasi yang selanjutnya disingkat TI telah memengaruhi cara kerja berbagai industri jasa keuangan, khususnya industri perbankan. Bank dapat memanfaatkan TI untuk mendukung kegiatan operasional Bank serta meningkatkan pelayanan kepada nasabah. Dengan menggunakan TI, Bank dapat memperoleh manfaat, antara lain peningkatan efisiensi dan efektivitas operasional Bank, peningkatan layanan melalui kerja sama dengan pihak ketiga secara mudah, serta penyediaan layanan yang cepat dan optimal bagi nasabah. Namun demikian, peningkatan pemanfaatan TI juga berpotensi meningkatkan risiko operasional bagi industri perbankan.

   Salah satu risiko yang berpotensi meningkat seiring dengan pemanfaatan TI pada skala yang lebih besar yaitu risiko yang ditimbulkan oleh ancaman dan insiden siber. Bank tidak hanya dituntut untuk dapat menjaga keamanan Sistem Elektronik yang

dimiliki dari serangan siber, namun juga perlu untuk memiliki kemampuan dalam mendeteksi dan memulihkan keadaan pasca terjadinya insiden siber.

Bank menerapkan tata kelola serta manajemen risiko yang baik untuk tetap dapat beroperasi dengan memanfaatkan TI sebagaimana mestinya dengan menjaga ketahanan dan keamanan siber. Selanjutnya, Bank juga perlu menetapkan strategi dan langkah yang tepat sasaran serta berkelanjutan dalam mengatasi permasalahan yang diakibatkan oleh ancaman dan insiden siber. Hal tersebut harus dilakukan mengingat bisnis perbankan merupakan bisnis yang utamanya berkaitan dengan dana masyarakat sehingga memerlukan operasional yang matang dan aman.

2. Ketahanan siber merupakan kemampuan Bank untuk tetap menjaga kelangsungan bisnisnya dengan melakukan tindakan antisipatif, adaptif, dan proaktif terhadap ancaman siber.
3. Keamanan siber merupakan kondisi terjaganya kerahasiaan, keutuhan, serta ketersediaan informasi dan/atau sistem informasi yang saling terkoneksi satu sama lain melalui media siber, dari serangan siber. Keamanan siber dapat juga mencakup aspek lain, seperti keaslian, akuntabilitas, nirsangkal, dan keandalan.
4. Laporan insiden TI berupa insiden siber yang selanjutnya disebut laporan insiden siber merupakan laporan kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI, yang terkait dengan keamanan siber.
5. Notifikasi awal insiden TI berupa insiden siber yang selanjutnya disebut notifikasi awal insiden siber merupakan pemberitahuan segera atas kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI, yang terkait dengan keamanan siber.

II. PENILAIAN RISIKO INHEREN TERKAIT KEAMANAN SIBER

1. Bank melakukan penilaian risiko inheren terkait keamanan siber. Penilaian tersebut dilakukan secara tahunan untuk posisi akhir bulan Desember. Bank dapat melakukan penginian penilaian tersebut sewaktu-waktu apabila diperlukan.
2. Penilaian risiko inheren terkait keamanan siber dilakukan dengan memperhatikan paling sedikit 4 (empat) faktor penilaian yaitu

teknologi, produk bank, karakteristik organisasi, dan rekam jejak insiden siber. Penilaian risiko inheren diawali dari penilaian terhadap parameter risiko pada setiap faktor penilaian terkait keamanan siber. Terdapat beberapa parameter atau indikator minimum yang dapat dijadikan acuan oleh Bank dalam menilai risiko inheren terkait keamanan siber sebagaimana tercantum dalam Lampiran I.a yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini. Bank dapat menambah parameter atau indikator lain yang relevan dengan karakteristik dan kompleksitas usaha Bank dengan memperhatikan prinsip proporsionalitas.

3. Dalam melakukan penilaian risiko inheren terkait keamanan siber, Bank menggunakan format sebagaimana tercantum dalam Lampiran II.a yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
4. Penetapan tingkat risiko inheren terkait keamanan siber dikategorikan ke dalam Peringkat 1 (*low*), Peringkat 2 (*low to moderate*), Peringkat 3 (*moderate*), Peringkat 4 (*moderate to high*), dan Peringkat 5 (*high*), sebagaimana tercantum dalam Lampiran III.a yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
5. Hasil penilaian risiko inheren terkait keamanan siber sebagaimana dimaksud pada angka 3 dan tingkat risiko inheren terkait keamanan siber sebagaimana dimaksud pada angka 4 disampaikan kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank, yaitu paling lama 15 (lima belas) hari kerja setelah akhir tahun pelaporan dengan menggunakan format sebagaimana tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
6. Penilaian risiko inheren terkait keamanan siber pertama kali dilakukan oleh Bank untuk posisi akhir bulan Desember 2022 dan hasil penilaian dimaksud disampaikan kepada Otoritas Jasa Keuangan paling lambat pada akhir bulan Juni 2023. Untuk penilaian tahun berikutnya disampaikan sesuai dengan tenggat waktu sebagaimana dimaksud pada angka 5.

7. Otoritas Jasa Keuangan melakukan penelaahan atas hasil penilaian risiko inheren terkait keamanan siber sebagaimana dimaksud pada angka 5. Dalam hal berdasarkan penelaahan Otoritas Jasa Keuangan menunjukkan bahwa hasil penilaian risiko inheren terkait keamanan siber tidak mencerminkan kondisi Bank yang sebenarnya, Otoritas Jasa Keuangan dapat menyesuaikan hasil penilaian risiko inheren terkait keamanan siber.
8. 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.

III. PENERAPAN MANAJEMEN RISIKO TERKAIT KEAMANAN SIBER

1. Untuk melaksanakan Pasal 15 POJK PTI, Bank menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI, termasuk terkait keamanan siber.
2. Penerapan manajemen risiko terkait keamanan siber mencakup 4 (empat) aspek, yaitu:
   a. tata kelola risiko terkait keamanan siber, yang meliputi kecukupan pengawasan aktif oleh Direksi dan Dewan Komisaris, perumusan tingkat risiko terkait keamanan siber yang akan diambil (*risk appetite*) dan toleransi risiko terkait keamanan siber (*risk tolerance*), serta budaya dan kesadaran risiko terkait keamanan siber;
   b. kerangka manajemen risiko terkait keamanan siber, yang meliputi strategi manajemen risiko, kecukupan perangkat organisasi, serta kecukupan kebijakan, prosedur, dan penetapan limit risiko, terkait keamanan siber;
   c. proses manajemen risiko, kecukupan sumber daya manusia (SDM), serta kecukupan sistem informasi manajemen risiko, terkait keamanan siber; dan
   d. sistem pengendalian risiko terkait keamanan siber, yang meliputi kecukupan sistem pengendalian intern dan kecukupan kaji ulang.
3. Penerapan manajemen risiko terkait keamanan siber disesuaikan dengan karakteristik dan kompleksitas bisnis Bank serta penyelenggaraan TI secara menyeluruh oleh Bank.

IV. PENERAPAN PROSES KETAHANAN SIBER BAGI BANK UMUM

1. Untuk melaksanakan Pasal 21 POJK PTI, Bank menjaga ketahanan siber dengan melakukan proses:
   a. identifikasi aset, ancaman, dan kerentanan;
   b. pelindungan aset;
   c. deteksi insiden siber; dan
   d. penanggulangan dan pemulihan insiden siber.
2. Proses Identifikasi Aset, Ancaman, dan Kerentanan

   Pada proses identifikasi aset, ancaman, dan kerentanan, Bank paling sedikit:
   a. menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta pencatatan konfigurasi secara efektif;
   b. melakukan identifikasi kerentanan dan pemantauan terhadap perkembangan siber terkini untuk mengidentifikasi ancaman siber; dan
   c. melakukan pengujian keamanan siber secara berkala.
3. Proses Pelindungan Aset

   Pada proses pelindungan aset, Bank paling sedikit:
   a. menerapkan pengendalian keamanan (*security control*) yang komprehensif sesuai dengan hasil identifikasi aset, ancaman, dan kerentanan sebagaimana dimaksud pada angka 2;
   b. melakukan pemeliharaan dan perbaikan terhadap pengendalian keamanan atas aset TI sesuai dengan kebijakan dan prosedur yang berlaku;
   c. menerapkan sistem pengamanan yang dikelola dengan baik sesuai kebijakan dan prosedur yang berlaku;
   d. melakukan penginian pengendalian keamanan Bank secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan sesuai dengan hasil terkini dari proses identifikasi;
   e. menerapkan manajemen keamanan data dan informasi serta memastikan bahwa data dan/atau informasi dikelola sesuai dengan strategi manajemen risiko organisasi untuk melindungi kerahasiaan, integritas, serta ketersediaan data dan informasi;
   f. menerapkan manajemen pelindungan terhadap jaringan, perangkat keras, dan perangkat lunak;

g. menerapkan manajemen pelindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastruktur jaringan, dan komponen sistem yang dikelola oleh Bank;

h. menerapkan pelindungan yang memadai dalam pelaksanaan kerja sama antara Bank dengan pihak penyedia jasa TI, termasuk dalam penggunaan *cloud*;

i. memastikan penerapan *secure coding* dalam pengembangan sistem dan aplikasi untuk meminimalisasi kerentanan atas sistem dan aplikasi; dan

j. memastikan pelaksanaan *patching* berjalan dengan baik serta memastikan keandalan dan kemutakhiran seluruh komponen perangkat lunak, jaringan komunikasi, *database*, dan sistem operasi (*operating system*) Bank.

4. Proses Deteksi Insiden Siber

Pada proses deteksi insiden siber, Bank paling sedikit:

a. memastikan ketersediaan dokumentasi kinerja dasar (*baseline performance*) atas fungsi kritis Bank dan sistem pendukung, agar setiap penyimpangan dapat dideteksi secara tepat waktu serta aktivitas dan kejadian anomali dapat ditandai untuk ditindaklanjuti;

b. melakukan pemantauan atas aktivitas mencurigakan serta melakukan pengelolaan dan pengujian terhadap proses dan prosedur deteksi untuk memastikan aktivitas anomali dapat dideteksi secara tepat waktu;

c. melakukan pemantauan atau deteksi secara berkelanjutan terhadap kerentanan untuk memastikan efektivitas upaya pelindungan yang telah diterapkan;

d. memastikan ketersediaan proses untuk mendeteksi insiden siber secara memadai; dan

e. melakukan analisis terhadap ancaman dan kerentanan dari suatu insiden siber untuk memastikan penanganan insiden secara efektif sehingga dapat mencegah terjadinya gangguan pada layanan dan/atau operasional Bank.

5. Proses Penanggulangan dan Pemulihan Insiden Siber

Pada proses penanggulangan dan pemulihan insiden siber, Bank paling sedikit:

a. menetapkan rencana penanggulangan dan pemulihan insiden siber untuk memastikan penanggulangan dan pengembalian layanan yang tepat waktu sesuai dengan risiko yang ditimbulkan, dengan dampak minimal;
b. menetapkan peran serta tugas dan tanggung jawab tim tanggap insiden siber untuk memastikan penanggulangan dan pemulihan insiden siber dilaksanakan dengan dampak minimal terhadap layanan dan operasional Bank;
c. menerapkan prosedur pemulihan dan upaya untuk mencegah penyebaran dampak dari suatu insiden siber dengan memitigasi dampak dan menanggulangi insiden siber tersebut;
d. melakukan analisis untuk memastikan langkah penanggulangan dan pemulihan insiden siber dijalankan dengan tepat;
e. melakukan eskalasi dan pelaporan atas insiden siber sesuai dengan jalur komunikasi yang telah ditetapkan; dan
f. melakukan analisis pascainsiden sebagai bahan pelajaran terpetik (*lesson learned*) dalam penanggulangan dan pemulihan insiden siber untuk perbaikan berkelanjutan.

V. PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

1. Penilaian maturitas keamanan siber bertujuan untuk mengukur tingkat maturitas yang telah dicapai oleh Bank. Tingkat maturitas keamanan siber mencerminkan kondisi keamanan siber pada Bank. Dalam hal teridentifikasi terdapat area yang memiliki kelemahan dan memerlukan perbaikan, hal tersebut dapat menjadi masukan dalam meningkatkan ketahanan dan keamanan siber Bank.
2. Tata Cara Penilaian Tingkat Maturitas Keamanan Siber
   a. Bank melakukan penilaian tingkat maturitas keamanan siber. Penilaian tersebut dilakukan secara tahunan untuk posisi akhir bulan Desember. Bank dapat melakukan penginian penilaian tersebut sewaktu-waktu apabila diperlukan.
   b. Penilaian tingkat maturitas keamanan siber mencakup penilaian terhadap:
      1) kualitas penerapan manajemen risiko terkait keamanan siber, yang meliputi aspek:
         a. tata kelola risiko terkait keamanan siber;

b. kerangka manajemen risiko terkait keamanan siber;
c. proses manajemen risiko, kecukupan SDM, dan kecukupan sistem informasi manajemen risiko, terkait keamanan siber; dan
d. sistem pengendalian risiko terkait keamanan siber;

2) kualitas penerapan proses ketahanan siber, yang meliputi proses:
a. identifikasi aset, ancaman, dan kerentanan;
b. pelindungan aset;
c. deteksi insiden siber; dan
d. penanggulangan dan pemulihan insiden siber.

c. Dalam menilai tingkat kualitas penerapan manajemen risiko terkait keamanan siber dan kualitas penerapan proses ketahanan siber sebagaimana dimaksud pada huruf b, Bank melakukan analisis terhadap penerapan kontrol sebagaimana tercantum dalam Lampiran I.b dan Lampiran I.c yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

d. Dalam melakukan penilaian tingkat maturitas keamanan siber, Bank menggunakan format sebagaimana tercantum dalam Lampiran II.b dan Lampiran II.c yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

e. Penetapan tingkat kualitas sebagaimana dimaksud pada huruf c dikategorikan ke dalam Peringkat 1 (*Strong*), Peringkat 2 (*Satisfactory*), Peringkat 3 (*Fair*), Peringkat 4 (*Marginal*), dan Peringkat 5 (*Unsatisfactory*) dilakukan dengan mengacu pada definisi peringkat sebagaimana tercantum dalam:

1) Lampiran III.b bagi penerapan manajemen risiko terkait keamanan siber; dan
2) Lampiran III.c bagi penerapan proses ketahanan siber,

yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

f. Penetapan tingkat maturitas keamanan siber dikategorikan ke dalam 5 (lima) tingkat, yaitu Tingkat 1, Tingkat 2, Tingkat 3, Tingkat 4, dan Tingkat 5 dilakukan dengan mengacu pada definisi peringkat sebagaimana tercantum dalam

Lampiran III.d yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

3. Hasil penilaian tingkat maturitas keamanan siber sebagaimana dimaksud pada angka 2 huruf d dan tingkat maturitas keamanan siber sebagaimana dimaksud pada 2 huruf f disampaikan kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank, yaitu paling lama 15 (lima belas) hari kerja setelah akhir tahun pelaporan menggunakan format sebagaimana tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
4. Penilaian tingkat maturitas keamanan siber pertama kali dilakukan oleh Bank untuk posisi akhir bulan Desember 2022 dan hasil penilaian dimaksud disampaikan kepada Otoritas Jasa Keuangan paling lambat pada akhir bulan Juni 2023. Untuk penilaian tahun berikutnya disampaikan sesuai dengan tenggat waktu sebagaimana dimaksud pada angka 3.
5. Otoritas Jasa Keuangan melakukan penelaahan atas hasil penilaian tingkat maturitas keamanan siber sebagaimana dimaksud pada angka 3. Dalam hal berdasarkan penelaahan Otoritas Jasa Keuangan menunjukkan bahwa hasil penilaian tingkat maturitas keamanan siber tidak mencerminkan kondisi Bank yang sebenarnya, Otoritas Jasa Keuangan dapat menyesuaikan hasil penilaian tingkat maturitas keamanan siber.
6. 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.

VI. TINGKAT RISIKO TERKAIT KEAMANAN SIBER

1. Tingkat risiko terkait keamanan siber ditetapkan berdasarkan penilaian risiko inheren terkait keamanan siber dan tingkat maturitas keamanan siber.
2. Penetapan tingkat risiko terkait keamanan siber dikategorikan ke dalam Peringkat 1 (*low*), Peringkat 2 (*low to moderate*), Peringkat 3 (*moderate*), Peringkat 4 (*moderate to high*), dan Peringkat 5 (*high*). Urutan peringkat tingkat risiko terkait keamanan siber yang lebih

kecil mencerminkan semakin rendahnya risiko terkait keamanan siber yang dihadapi oleh Bank.

3. Tingkat risiko terkait keamanan siber sebagaimana dimaksud pada angka 1 disampaikan kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank, yaitu paling lama 15 (lima belas) hari kerja setelah akhir tahun pelaporan menggunakan format sebagaimana tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
4. Penetapan tingkat risiko terkait keamanan siber pertama kali dilakukan oleh Bank untuk posisi akhir bulan Desember 2022 dan disampaikan kepada Otoritas Jasa Keuangan paling lambat pada akhir bulan Juni 2023. Untuk tahun berikutnya, tingkat risiko terkait keamanan siber disampaikan sesuai dengan tenggat waktu sebagaimana dimaksud pada angka 3.
5. Otoritas Jasa Keuangan melakukan penelaahan atas tingkat risiko terkait keamanan siber sebagaimana dimaksud pada angka 2. Dalam hal berdasarkan penelaahan Otoritas Jasa Keuangan menunjukkan bahwa tingkat risiko terkait keamanan siber tidak mencerminkan kondisi Bank yang sebenarnya, Otoritas Jasa Keuangan dapat menyesuaikan hasil penetapan tingkat risiko terkait keamanan siber.

VII. PENGUJIAN KEAMANAN SIBER

1. Bank melakukan pengujian keamanan siber secara berkala atas keamanan jaringan, sistem, dan data sebagai langkah untuk memaksimalkan upaya menjaga keamanan siber Bank. Pengujian keamanan siber terbagi menjadi 2 (dua) yaitu pengujian keamanan siber berdasarkan:
   a. analisis kerentanan; dan
   b. skenario.
2. Pengujian Keamanan Siber Berdasarkan Analisis Kerentanan
   Bank melakukan pengujian keamanan siber berdasarkan analisis kerentanan untuk melihat titik lemah dari sistem Bank. Pengujian ini dilaksanakan secara berkala berdasarkan evaluasi intern Bank. Contoh faktor yang dapat mendasari penentuan frekuensi pengujian ini yaitu tingkat kritikalitas sistem dari hasil identifikasi

aset TI Bank dan adanya perubahan pada Sistem Elektronik atau arsitektur TI pada Bank yang mengakibatkan peningkatan eksposur risiko terkait keamanan siber. Pengujian ini diawali dengan pelaksanaan identifikasi kerentanan yang kemudian dilanjutkan dengan *penetration test*.

Penetration test merupakan pengujian yang menggunakan serangkaian teknik dan metodologi dengan memanfaatkan sumber daya yang tersedia, antara lain *source code*, desain sistem, dan manual sistem Bank. *Penetration test* bertujuan untuk menerobos sistem pengamanan yang ada, sesuai dengan batasan yang telah ditentukan sebelumnya. Selanjutnya, *penetration test* perlu dilakukan secara berkala pada perangkat lunak dan perangkat keras yang digunakan oleh Bank, baik untuk operasional maupun layanan kepada nasabah dan/atau pihak ketiga. Secara khusus, pengujian ini harus dilakukan oleh Bank yang menyelenggarakan layanan perbankan digital atau layanan lain yang beroperasi secara daring.

3. Pengujian Keamanan Siber Berdasarkan Skenario

   Pengujian keamanan siber berdasarkan skenario perlu dilakukan oleh Bank untuk memvalidasi proses penanggulangan dan pemulihan insiden siber pada Bank, termasuk rencana komunikasi Bank dalam menghadapi ancaman siber. Dalam pelaksanaan pengujian ini, Bank harus melibatkan pihak yang relevan, termasuk pejabat eksekutif, fungsi bisnis, fungsi komunikasi korporasi, tim manajemen krisis, penyedia layanan, dan staf teknis yang bertanggung jawab atas proses deteksi insiden siber, serta proses penanggulangan dan pemulihan insiden siber. Beberapa jenis pengujian keamanan siber berdasarkan skenario yang dapat dilakukan oleh Bank antara lain *table-top exercise, cyber range exercise, social engineering exercise,* dan *adversarial attack simulation exercise*.

   a. *Table-top Exercise*

      Table-top exercise merupakan suatu kegiatan berbasis diskusi dimana SDM dengan peran dan tanggung jawab tertentu pada Bank bertemu dalam suatu forum untuk mendiskusikan peran masing-masing selama keadaan darurat dan penanggulangan yang dilakukan terhadap situasi darurat tertentu. Dalam

pelaksanaannya, terdapat fasilitator yang memandu peserta melalui diskusi yang dirancang untuk memenuhi tujuan yang telah ditentukan sebelumnya.

b. *Cyber Range Exercise*

Cyber range exercise merupakan pengujian yang menggunakan representasi simulasi yang interaktif atas jaringan, sistem, perangkat, dan aplikasi dari Bank. Simulasi tersebut memungkinkan pelaksanaan pengujian pada lingkungan yang terkendali serta tidak mengganggu kelangsungan operasional Bank.

c. *Social Engineering Exercise*

Social engineering exercise merupakan pengujian dengan menggunakan skenario dimana penyerang memanipulasi pegawai yang kurang waspada untuk membocorkan informasi sensitif seperti kata sandi, melalui penggunaan teknik seperti *phishing* dan *spam*. Pengujian ini dapat dilakukan untuk mengetahui tingkat kesadaran (*awareness*) terhadap keamanan siber dari pegawai.

d. *Adversarial Attack Simulation Exercise*

Adversarial Attack Simulation Exercise (AASE) merupakan pengujian yang menggunakan simulasi taktik, teknik, dan prosedur dari serangan siber di dunia nyata untuk menargetkan SDM, proses, dan teknologi yang mendukung fungsi kritis Bank. AASE memberikan gambaran yang lebih realistis tentang kemampuan organisasi untuk mencegah, mendeteksi, dan menanggulangi serangan. Dalam AASE umumnya terdapat *red team* dan *blue team*. *Red team* berperan sebagai penyerang yang melakukan simulasi serangan menggunakan taktik, teknik, dan prosedur dari serangan siber di dunia nyata. Sementara itu, *blue team* berperan sebagai pihak yang melakukan deteksi dan/atau pencegahan atas simulasi serangan yang dilakukan oleh *red team* dan menanggulangi insiden siber yang terjadi.

Hal yang perlu diperhatikan dalam pelaksanaan pengujian berdasarkan skenario, yaitu:

1) pengujian dalam bentuk simulasi serangan harus dilakukan secara terkendali di bawah pengawasan ketat untuk

memastikan pengujian tersebut tidak mengganggu sistem Bank di lingkungan produksi; dan

2) skenario ancaman harus dirancang dan didasarkan pada ancaman siber yang mungkin terjadi. Bank juga dapat merancang skenario melalui proses pencarian ancaman siber secara proaktif yang menyeluruh, antara lain dengan menggunakan *threat intelligence* yang relevan dengan lingkungan TI Bank untuk mengidentifikasi *threat actor* yang dapat menimbulkan ancaman siber bagi Bank, dan mengidentifikasi taktik, teknik, serta prosedur yang dapat digunakan dalam serangan tersebut.

4. Penyampaian Hasil Pengujian Keamanan Siber

a. Hasil pengujian keamanan siber disampaikan kepada Direksi sebagai landasan untuk perbaikan tata kelola, kebijakan dan prosedur, pengendalian intern, serta peningkatan kapasitas dan kesadaran (*awareness*) pegawai Bank terhadap ketahanan dan keamanan siber.

b. Bank juga menyampaikan hasil pengujian keamanan siber kepada Otoritas Jasa Keuangan, dengan ketentuan sebagai berikut:

1) Hasil pengujian keamanan siber berdasarkan analisis kerentanan sebagaimana dimaksud pada angka 2 disampaikan kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank, yaitu paling lama 15 (lima belas) hari kerja setelah akhir tahun pelaporan.

Contoh:

Bank melakukan beberapa *penetration test* di tahun 2022, antara lain pada bulan Maret 2022, Juli 2022, dan November 2022. Kompilasi hasil pengujian keamanan siber berupa *penetration test* tersebut disampaikan kepada Otoritas Jasa Keuangan paling lambat pada tanggal 20 Januari 2023, sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.

2) Hasil pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud pada angka 3 disampaikan kepada Otoritas Jasa Keuangan paling lama 10 (sepuluh)

hari kerja setelah pengujian keamanan siber selesai dilaksanakan, sesuai dengan format sebagaimana tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini. Pengujian keamanan siber dianggap selesai dilaksanakan pada saat laporan hasil pengujian selesai disusun.

Hasil pengujian keamanan siber paling sedikit memuat:

a) ringkasan pelaksanaan pengujian;
b) pelajaran terpetik (*lesson learned*) atau hasil observasi dari hasil pengujian; dan
c) rencana atau perbaikan yang telah dilakukan.

Contoh:

Bank melakukan pengujian keamanan siber dengan skenario serangan berupa *ransomware* pada tanggal 3 November 2023. Selanjutnya, pengujian tersebut selesai dilakukan dan laporan hasil pengujian telah selesai disusun pada tanggal 14 November 2023. Hasil pengujian keamanan siber tersebut disampaikan kepada Otoritas Jasa Keuangan paling lambat pada tanggal 28 November 2023.

5. Bank dapat melakukan pengujian keamanan siber secara mandiri atau menggunakan pihak ketiga. Dalam hal pengujian keamanan siber menggunakan pihak ketiga, Bank harus:
   a. memastikan pihak ketiga memiliki kompetensi yang memadai sesuai dengan kebutuhan pengujian keamanan siber; dan
   b. tetap bertanggung jawab atas pelaksanaan pengujian keamanan siber.

   Kompetensi dari pihak ketiga dibuktikan antara lain dengan adanya sertifikasi dan/atau pengakuan dari lembaga yang berwenang di Indonesia atau di luar negeri.
6. Pengujian keamanan siber pertama kali dilakukan oleh Bank pada tahun 2023.
7. Bank melakukan dokumentasi dan pengamanan yang memadai atas hasil pengujian keamanan siber yang telah dilakukan untuk menjaga kerahasiaan hasil pengujian keamanan siber.

VIII. UNIT ATAU FUNGSI YANG MENANGANI KETAHANAN DAN KEAMANAN SIBER BANK

1. Bank membentuk unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber Bank.
2. Unit atau fungsi yang menangani ketahanan dan keamanan siber memiliki tugas untuk mengoordinasikan dan/atau melaksanakan:
   a. proses ketahanan siber Bank sebagaimana dimaksud pada romawi IV;
   b. penilaian sendiri atas risiko inheren terkait keamanan siber sebagaimana dimaksud pada romawi II dan tingkat maturitas keamanan siber sebagaimana dimaksud pada romawi V;
   c. penetapan tingkat risiko terkait keamanan siber sebagaimana dimaksud pada romawi VI; dan
   d. pengujian keamanan siber sebagaimana dimaksud pada romawi VII.
3. Unit atau fungsi yang menangani ketahanan dan keamanan siber Bank memiliki independensi terhadap fungsi pengelolaan TI. Fungsi pengelolaan TI dimaksud paling sedikit berupa aktivitas perencanaan, penyusunan atau pengembangan, pengoperasian, dan pemantauan, atas kegiatan penyelenggaraan TI.
4. Unit atau fungsi yang menangani ketahanan dan keamanan siber mengoordinasikan tim tanggap insiden siber, termasuk inisasi pembentukannya, dengan memastikan bahwa:
   a. pegawai yang terlibat dalam tim tanggap insiden siber memiliki kapasitas dan kemampuan terkait penanganan insiden siber, yaitu dengan melakukan latihan respons insiden secara rutin, antara lain berupa pengujian saluran komunikasi, analisis insiden, pengambilan keputusan dan rekomendasi solusi, serta kemampuan teknis pelaporan insiden;
   b. tim tanggap insiden siber dapat bekerja sama dengan unit atau fungsi terkait (antara lain spesialis keamanan teknis, unit bisnis, fungsi hukum, SDM, dan tim komunikasi ekstern) dan mampu mengakses informasi yang diperlukan dengan cepat (antara lain informasi dari penyedia jasa pihak ketiga atau informasi pendukung lainnya);
   c. tim tanggap insiden siber memiliki sumber daya analisis insiden (antara lain daftar *host, packet sniffer*, analisis

protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, perangkat forensik digital, dan sumber daya lain yang diperlukan);

d. tim tanggap insiden siber dapat bekerja sama secara efektif dengan fungsi intelijen ancaman siber *(cyber threat intelligence)* dan *network operations* untuk menghasilkan penanganan insiden siber yang tepat dan proaktif terhadap potensi insiden siber di masa depan;

e. tim tanggap insiden siber dipimpin oleh pejabat yang berasal dari unit atau fungsi yang menangani ketahanan dan keamanan siber; dan

f. tim tanggap insiden siber memiliki narahubung untuk mendukung koordinasi dalam pelaksanaan tugas.

IX. LAPORAN INSIDEN SIBER

1. Insiden TI merupakan kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI. Insiden TI terbagi menjadi 2 (dua) kategori yaitu insiden siber dan insiden nonsiber.

2. Insiden siber terjadi karena terganggunya keamanan siber. Insiden siber merupakan ancaman siber berupa upaya, kegiatan, dan/atau tindakan yang mengakibatkan Sistem Elektronik tidak berfungsi sebagaimana mestinya. Beberapa contoh ancaman siber:

   a. *Malware*

      Malware merupakan perangkat lunak dengan fitur atau kemampuan yang berpotensi mengganggu suatu sistem informasi. Gangguan dimaksud dapat menimbulkan kerugian bagi pemilik sistem informasi, baik secara langsung maupun tidak langsung.

   b. *Web defacement*

      Web d*efacement* merupakan serangan yang dilakukan terhadap situs web dengan cara mengganti atau memodifikasi situs web sehingga isi dari situs web berubah sesuai dengan keinginan penyerang.

   c. *Denial of Services* (DoS) dan *Distributed Denial of Services* (DDoS)

      DoS dan DDoS merupakan serangan yang bertujuan untuk mengganggu keberlangsungan operasional (*availability*) suatu

Sistem Elektronik dalam memproses transaksi atau akses yang sah, antara lain dengan cara membuat kapasitas jaringan atau kapasitas komputer seolah-olah telah terpakai penuh karena adanya permintaan akses dalam volume yang besar.

3. Bank perlu melakukan pemantauan atas insiden siber sebagai bentuk komunikasi kepada para pemangku kepentingan serta pengendalian atas pengelolaan ketahanan dan keamanan siber. Kegiatan pemantauan insiden siber dapat bermanfaat bagi Bank dalam melakukan penanggulangan dan pemulihan terhadap Sistem Elektronik Bank, sehingga kegiatan operasional Bank tetap dapat berjalan sebagaimana mestinya.
4. Bank menyampaikan informasi mengenai insiden siber kepada Otoritas Jasa Keuangan berupa:
   a. notifikasi awal insiden siber; dan
   b. laporan insiden siber.
5. Notifikasi awal insiden siber disampaikan oleh Bank dengan ketentuan sebagai berikut:
   a. Notifikasi awal disusun menggunakan format sebagaimana tercantum dalam Lampiran IV.a yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini. Notifikasi awal berisi informasi awal yang tersedia terkait insiden siber pada Bank.
   b. Notifikasi awal disampaikan kepada Otoritas Jasa Keuangan paling lama 24 (dua puluh empat) jam setelah insiden siber diketahui oleh Bank, ditujukan kepada pengawas Bank yang bersangkutan melalui sarana elektronik secara tertulis. Bank melakukan upaya untuk memastikan bahwa notifikasi awal telah diterima oleh Otoritas Jasa Keuangan.
6. Sebagai tindak lanjut dari notifikasi awal insiden siber yang telah disampaikan, Bank melakukan analisis dan penanggulangan insiden siber lebih lanjut. Tindak lanjut ini disampaikan melalui laporan insiden siber kepada Otoritas Jasa Keuangan dengan ketentuan sebagai berikut:
   a. Laporan insiden siber disusun menggunakan format sebagaimana tercantum dalam Lampiran IV.b yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini. Laporan insiden siber berisi informasi yang lebih

lengkap dari informasi yang telah disampaikan pada notifikasi awal.

b. Laporan insiden siber disampaikan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan paling lama 5 (lima) hari kerja setelah insiden siber diketahui.

7. Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal dan/atau laporan insiden siber, Bank menyampaikan notifikasi awal dan/atau laporan insiden siber kepada Otoritas Jasa Keuangan dengan ketentuan sebagai berikut:

a. Dalam hal otoritas lain mengatur jangka waktu penyampaian notifikasi awal dan/atau laporan insiden siber lebih cepat dari jangka waktu sebagaimana diatur dalam POJK PTI maka Bank menyampaikan notifikasi awal dan/atau laporan insiden siber kepada Otoritas Jasa Keuangan pada saat yang bersamaan sesuai dengan ketentuan peraturan perundang-undangan dari otoritas lain dimaksud.

Contoh:

Ketentuan Otoritas “A”

Jangka waktu penyampaian notifikasi awal insiden siber.	Paling lama 1 (satu) jam setelah insiden siber diketahui.
Jangka waktu penyampaian laporan insiden siber.	Paling lama 3 (tiga) hari kerja setelah insiden siber diketahui.

Bank “B” mengalami insiden siber pada tanggal 22 Agustus 2023 pukul 13.00 WITA. Mengingat jangka waktu penyampaian notifikasi awal dan/atau laporan insiden siber berdasarkan ketentuan otoritas “A” lebih cepat daripada yang diatur dalam POJK PTI, maka Bank “B” menyampaikan notifikasi awal dalam kurun waktu 1 (satu) jam setelah insiden siber diketahui. Apabila Bank “B” menyampaikan notifikasi awal insiden siber kepada otoritas “A” pada pukul 13.45 WITA maka Bank “B” juga menyampaikan notifikasi awal kepada Otoritas Jasa Keuangan pada saat yang bersamaan.

Hal yang sama juga berlaku untuk penyampaian laporan insiden siber. Apabila Bank "B" menyampaikan laporan insiden siber pada tanggal 24 Agustus 2023 pukul 10.00 WITA kepada otoritas "A" maka Bank "B" juga menyampaikan laporan insiden siber kepada Otoritas Jasa Keuangan pada saat yang bersamaan.

b. Apabila otoritas lain mengatur jangka waktu penyampaian notifikasi awal dan/atau laporan insiden siber lebih lama dari jangka waktu sebagaimana diatur dalam POJK PTI, maka Bank menyampaikan notifikasi awal dan/atau laporan insiden siber kepada Otoritas Jasa Keuangan sesuai dengan POJK PTI.

Contoh:

Ketentuan Otoritas "C"

Jangka waktu penyampaian notifikasi awal insiden siber.	Paling lama 3 (tiga) hari kerja setelah insiden siber diketahui.
Jangka waktu penyampaian laporan insiden siber.	Paling lama 10 (sepuluh) hari kerja setelah insiden siber diketahui.

Bank "D" mengalami insiden siber pada tanggal 22 Agustus 2023 pukul 13.00 WITA. Mengingat jangka waktu penyampaian notifikasi awal dan/atau laporan insiden siber berdasarkan POJK PTI lebih cepat daripada yang diatur dalam ketentuan otoritas "C" maka Bank "D" menyampaikan notifikasi awal kepada Otoritas Jasa Keuangan dalam kurun waktu 24 (dua puluh empat) jam setelah insiden siber diketahui.

Hal yang sama juga berlaku untuk penyampaian laporan insiden siber. Bank "D" menyampaikan laporan insiden siber kepada Otoritas Jasa Keuangan dalam kurun waktu 5 (lima) hari kerja setelah insiden siber diketahui.

X. PENUTUP

Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN I

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

I.a. Penilaian Risiko Inheren terkait Keamanan Siber

Matriks Parameter atau Indikator Penilaian Risiko Inheren terkait Keamanan Siber

No.	Parameter atau Indikator		Keterangan
1.	Teknologi	1.1. Interkoneksi ke internet publik.	Jumlah interkoneksi Bank ke internet publik memengaruhi risiko inheren Bank. Semakin banyak jumlah interkoneksi maka semakin tinggi risiko inheren Bank.
		1.2. Interkoneksi ke pihak ketiga (*third party*).	Terdapat beberapa tipe koneksi dari Bank ke pihak ketiga, yaitu: a. *Direct connection* (*clear channel*/*link*/MLPLS/*Internet Protocol* (*IP) Based*) (*Open System Interconnection* (OSI) *Layer* 3); b. *Host to Host* – FTP/SFTP (OSI *Layer* 4); dan c. *Application Programming Interface*/API (OSI *Layer* 7). Penggunaan tipe koneksi memengaruhi risiko inheren Bank. Semakin banyak penggunaan tipe koneksi dengan OSI *Layer* rendah (seperti *direct connection*) maka semakin tinggi risiko inheren Bank.
		1.3. Akses ke aset TI Bank.	Akses ke aset TI Bank dapat dilihat dari 2 (dua) sisi, yaitu metode yang digunakan dan pihak yang mengakses. Metode yang digunakan dapat berupa koneksi nirkabel atau koneksi kabel. Sementara itu, pihak yang melakukan akses dapat berupa pegawai, pihak ketiga (*third party*), atau publik (tamu atau nasabah). Kebijakan Bank mengenai pihak yang dapat melakukan akses ke aset TI Bank serta metode yang digunakan memengaruhi risiko inheren Bank. Semakin banyak pihak yang dapat mengakses aset TI Bank maka semakin tinggi risiko inheren Bank.
		1.4. Jaringan intranet dari jaringan kantor Bank.	Akses langsung dari jaringan kantor ke *core system* melalui intranet memengaruhi risiko inheren Bank. Jaringan kantor sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai bank umum termasuk antara lain kantor pusat, kantor wilayah, kantor cabang, dan kantor cabang pembantu. Semakin banyak jumlah jaringan kantor yang memiliki akses ke *core system* maka semakin tinggi risiko inheren Bank.

No.	Parameter atau Indikator		Keterangan
		1.5. Penggunaan pihak penyedia jasa TI dalam penyelenggaraan pusat data.	Bentuk penyediaan jasa TI dapat berupa: a. *cloud service*, seperti *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), dan *Software as a Service* (SaaS); dan/atau b. non-*cloud service*, seperti *colocation*. Penggunaan *cloud service* memberikan risiko inheren yang lebih tinggi dibandingkan penggunaan penyediaan jasa teknologi non-*cloud service*.
		1.6. Pengelolaan perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* dan TI).	Pengelolaan perangkat lunak yaitu pengembangan dan penyelenggaraan atas perangkat lunak tersebut. Pengelolaan ini dapat dilakukan sendiri oleh Bank dan/atau menggunakan pihak ketiga. Semakin Bank bergantung pada pihak ketiga dalam pengelolaan perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank maka semakin tinggi risiko inheren Bank.
		1.7. Penggunaan perangkat keras dan/atau perangkat lunak yang sudah masuk/mendekati masa *End-of-life* (EOL).	Penggunaan perangkat keras dan/atau perangkat lunak yang sudah masuk/mendekati masa EOL memengaruhi risiko inheren Bank. Semakin banyak Bank menggunakan perangkat keras dan/atau perangkat lunak yang sudah masuk/mendekati masa EOL maka semakin tinggi risiko inheren Bank.
		1.8. Jumlah pegawai yang memiliki akses koneksi perangkat pribadi ke jaringan Bank (*Bring Your Own Device*).	Jumlah pegawai yang memiliki akses ke jaringan Bank melalui perangkat pribadi memengaruhi risiko inheren Bank. Semakin besar persentase pegawai yang memiliki akses melalui perangkat pribadi maka semakin tinggi risiko inheren Bank.
		1.9. Perangkat lunak yang dapat diakses menggunakan perangkat pribadi ke jaringan Bank.	Perangkat lunak intern Bank yang dapat diakses oleh perangkat pribadi terbagi menjadi 4 (empat), yaitu: a. aplikasi surat elektronik; b. aplikasi penunjang; c. aplikasi kritikal; dan d. *core banking system*.

No.	Parameter atau Indikator		Keterangan
			Semakin tinggi kritikalitas aplikasi yang dapat diakses oleh perangkat pribadi maka semakin tinggi risiko inheren Bank.
		1.10. Pihak ketiga yang memiliki akses terhadap sistem internal Bank dan/atau informasi sensitif.	Pihak ketiga dalam hal ini termasuk perusahaan (ekstern dan *intragroup*) dan individu dari vendor dan/atau subkontraktor. Jumlah pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif Bank memengaruhi risiko inheren Bank. Semakin banyak pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif Bank maka semakin tinggi risiko inheren Bank.
2.	Produk Bank	2.1. Penggunaan saluran daring dan *mobile* dalam memberikan layanan.	Saluran daring dan *mobile* dapat digunakan oleh Bank untuk: a. penyampaian informasi umum Bank kepada masyarakat (a.l. lokasi jaringan kantor, dan produk Bank yang tersedia); b. pelayanan transaksi perbankan (produk Bank); dan/atau c. interkoneksi dengan ekosistem ekonomi digital (*super app*). Semakin luas penggunaan saluran daring dan *mobile* yang dimiliki Bank maka semakin tinggi risiko inheren Bank.
		2.2. Mekanisme pengelolaan *Automated Teller Machine* (ATM).	Pengelolaan ATM Bank dapat dilakukan sendiri oleh Bank atau menggunakan pihak ketiga, atau kombinasi keduanya. Semakin besar peran pihak ketiga dalam pengelolaan ATM maka semakin tinggi risiko inheren Bank.
		2.3. Produk Bank berupa alat pembayaran menggunakan kartu (APMK).	Produk Bank berupa APMK memengaruhi risiko inheren Bank. Bank yang menerbitkan APMK memiliki risiko inheren yang lebih tinggi dibandingkan dengan Bank yang tidak menerbitkan APMK.
		2.4. Jenis produk Bank berbasis TI.	Jenis produk Bank yang berbasis TI memengaruhi risiko inheren Bank. Semakin banyak jenis produk Bank yang berbasis TI maka semakin tinggi risiko inheren Bank.
		2.5. Bank sebagai penyedia jasa TI.	Penyediaan jasa TI oleh Bank memengaruhi risiko inheren Bank. Semakin banyak Bank memberikan jasa TI kepada pihak lain maka semakin tinggi risiko inheren Bank.

No.	Parameter atau Indikator		Keterangan
3	Karakteristik Organisasi	3.1. Pergantian (*turnover*) pada SDM yang menangani TI/ketahanan dan keamanan siber.	Pergantian pada SDM di TI/ketahanan dan keamanan siber memengaruhi risiko inheren Bank. Semakin sering terjadi pergantian SDM maka semakin tinggi risiko inheren Bank.
		3.2. Perubahan di lingkungan TI.	Perubahan di lingkungan TI tercermin dari implementasi sistem kritikal pada Bank. Semakin banyak Bank mengimplementasikan sistem kritikal maka semakin tinggi risiko inheren Bank.
		3.3. Pengelolaan *privilege access* (administrator dan selevel administrator) di seluruh perangkat (*host*, jaringan, *database*, aplikasi, dan *cloud*).	Pengelolaan *privilege access* pada perangkat Bank memengaruhi risiko inheren Bank. Semakin banyak tipe perangkat yang dikelola oleh pihak selain unit TI maka semakin tinggi risiko inheren Bank.
4	Rekam Jejak Insiden Siber	4.1. Persentase insiden siber yang berdampak signifikan dalam 12 (dua belas) bulan terakhir.	Persentase insiden siber yang berdampak signifikan memengaruhi risiko inheren Bank. Semakin tinggi persentase insiden siber yang berdampak signifikan maka semakin tinggi risiko inheren Bank. Persentase insiden yang diperhitungkan merupakan insiden aktual yang terjadi di Bank, bukan hanya yang dilaporkan kepada Otoritas Jasa Keuangan. Signifikansi dari insiden dapat mempertimbangkan antara lain jenis data yang bocor, *down-time* aplikasi, dan dampak finansial yang terjadi.
		4.2. Cakupan dampak insiden siber dalam 12 (dua belas) bulan terakhir.	Dampak insiden siber memengaruhi risiko inheren Bank. Semakin kritikal dampak dari insiden siber yang terjadi maka semakin tinggi risiko inheren Bank.

I.b. Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber

Matriks Kontrol Penerapan Manajemen Risiko terkait Keamanan Siber

No.	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
1.	Tata Kelola Risiko terkait Keamanan Siber	1.1. Kecukupan Pengawasan Aktif oleh Direksi dan Dewan Komisaris	1.1.a. Bank menetapkan wewenang dan tanggung jawab Direksi terkait dengan penerapan manajemen risiko terkait keamanan siber.	Wewenang dan tanggung jawab Direksi paling sedikit: 1) memiliki tanggung jawab penuh atas penerapan manajemen risiko terkait keamanan siber Bank; 2) memastikan penerapan manajemen risiko terkait keamanan siber telah memadai sesuai dengan karakteristik, kompleksitas, dan profil risiko Bank; 3) memiliki pemahaman yang memadai mengenai jenis dan tingkat risiko terkait keamanan siber yang melekat pada Bank; 4) memastikan Bank memiliki SDM dan infrastruktur yang cukup untuk mendukung manajemen risiko terkait keamanan siber Bank; 5) mendukung terciptanya budaya manajemen risiko terkait keamanan siber dengan memberikan perhatian yang cukup terhadap pelaksanaan manajemen risiko terkait keamanan siber oleh seluruh elemen organisasi Bank; 6) menjadi contoh standar perilaku yang mengedepankan kesadaran (*awareness*) terhadap risiko terkait keamanan siber bagi pegawai dan seluruh elemen organisasi Bank; 7) melakukan pengawasan secara aktif atas penerapan manajemen risiko terkait keamanan siber; 8) menyusun dan menetapkan kebijakan, strategi, dan kerangka manajemen risiko terkait keamanan siber secara tertulis dan komprehensif termasuk

				limit risiko terkait keamanan siber dan melakukan pemantauan implementasi manajemen risiko terkait keamanan siber oleh Bank; 9) menyusun, menetapkan, dan menginikan prosedur untuk mengidentifikasi, mengukur, memonitor, dan mengendalikan risiko terkait keamanan siber; 10) melaksanakan kebijakan strategi dan kerangka manajemen risiko terkait keamanan siber yang telah disetujui oleh Dewan Komisaris serta mengevaluasi dan memberikan arahan berdasarkan laporan yang disampaikan oleh satuan kerja pelaksana, satuan kerja manajemen risiko, satuan kerja kepatuhan, dan satuan kerja audit intern; 11) mengevaluasi dan/atau menginikan kebijakan, strategi, dan kerangka manajemen risiko terkait keamanan siber serta melakukan internalisasi kerangka manajemen risiko terkait keamanan siber ke dalam kebijakan dan prosedur bisnis pada seluruh unit bisnis dan aktivitas pendukung; 12) menetapkan struktur organisasi, termasuk wewenang dan tanggung jawab yang jelas pada setiap jenjang jabatan yang terkait dengan penerapan manajemen risiko terkait keamanan siber; 13) memastikan kecukupan dukungan sumber daya untuk mengelola dan mengendalikan risiko terkait keamanan siber; 14) memastikan bahwa seluruh pegawai dengan peran dan tanggung jawab terkait keamanan siber memiliki keterampilan, pengetahuan, pengalaman,

				dan sumber daya yang memadai untuk melakukan tugas yang diperlukan secara efektif; 15) menugaskan pejabat yang memiliki keterampilan, pengetahuan, dan pengalaman yang sesuai untuk bertanggung jawab atas strategi keamanan siber Bank serta memimpin fungsi yang bertugas menangani penerapan manajemen risiko terkait keamanan siber dalam organisasi Bank; 16) memastikan bahwa pejabat yang ditunjuk dapat secara langsung melaporkan penerapan dan/atau permasalahan terkait keamanan siber kepada Direksi secara berkala, termasuk setiap perubahan pada titik kerentanan Bank atau perubahan pada ancaman siber; 17) memastikan seluruh risiko terkait keamanan siber yang material dan dampak yang ditimbulkan oleh risiko dimaksud telah ditindaklanjuti dan menyampaikan laporan pertanggungjawaban kepada Dewan Komisaris secara berkala, antara lain memuat laporan perkembangan dan permasalahan mengenai risiko terkait keamanan siber yang material disertai dengan langkah perbaikan yang telah, sedang, dan akan dilakukan; 18) memastikan pelaksanaan langkah perbaikan atas permasalahan atau penyimpangan terkait keamanan siber yang ditemukan; 19) memastikan bahwa fungsi manajemen risiko terkait keamanan siber telah diterapkan secara independen yang tercermin dari antara lain adanya pemisahan fungsi antara satuan kerja pelaksana dengan satuan kerja yang berfungsi untuk

				melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko terkait keamanan siber; 20) membentuk *change advisory board* yang bertugas untuk meninjau seluruh perubahan konfigurasi yang dilakukan dalam sistem Bank melalui *change management system* yang dikaji ulang secara berkala serta memberikan rekomendasi kepada Direksi untuk menyetujui terkait perubahan dimaksud; dan 21) memastikan kaji ulang terhadap rencana penanggulangan dan pemulihan insiden siber Bank dilaksanakan secara berkala.
			1.1.b. Bank menetapkan wewenang dan tanggung jawab Dewan Komisaris terkait dengan penerapan manajemen risiko terkait keamanan siber.	Wewenang dan tanggung jawab Dewan Komisaris paling sedikit: 1) memiliki pemahaman yang memadai mengenai jenis dan tingkat risiko terkait keamanan siber yang melekat pada Bank; 2) memastikan Bank memiliki SDM dan infrastruktur yang cukup untuk mendukung penerapan manajemen risiko terkait keamanan siber dan proses ketahanan siber Bank; 3) mendukung terciptanya budaya manajemen risiko terkait keamanan siber dengan memberikan perhatian yang cukup terhadap pelaksanaan manajemen risiko terkait keamanan siber oleh seluruh elemen organisasi Bank; 4) menjadi contoh standar perilaku yang mengedepankan kesadaran (*awareness*) terhadap risiko terkait keamanan siber bagi pegawai dan seluruh elemen organisasi Bank;

				5) melakukan pengawasan secara aktif atas penerapan manajemen risiko terkait keamanan siber; 6) menyetujui kebijakan dan rencana strategis terkait manajemen risiko terkait keamanan siber yang ditetapkan sesuai dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko Bank (*risk tolerance*); 7) mengevaluasi kebijakan manajemen risiko dan strategi risiko terkait keamanan siber secara berkala, paling sedikit satu kali dalam satu tahun atau lebih dalam hal terdapat perubahan faktor yang memengaruhi kegiatan usaha Bank secara signifikan; 8) mengevaluasi pertanggungjawaban Direksi dan memberikan arahan perbaikan atas pelaksanaan kebijakan manajemen risiko terkait keamanan siber secara berkala; dan 9) memastikan kebijakan dan proses manajemen risiko terkait keamanan siber dilaksanakan secara efektif dan terintegrasi dalam proses manajemen risiko secara keseluruhan.
		1.2. Perumusan Tingkat Risiko yang Akan Diambil (*Risk Appetite*)	1.2.a. Direksi bertanggung jawab untuk menetapkan tingkat risiko yang diambil (*risk appetite*) terkait keamanan siber Bank.	Tingkat risiko yang akan diambil merupakan tingkat risiko yang bersedia diambil oleh Bank dalam rangka mencapai sasaran tingkat kualitas penerapan manajemen risiko terkait keamanan siber Bank. Tingkat risiko yang akan diambil tercermin dalam

		dan Toleransi Risiko (*Risk Tolerance*) terkait Keamanan Siber	1.2.b. Direksi bertanggung jawab untuk menetapkan toleransi risiko (*risk tolerance*) terkait keamanan siber Bank.	strategi dan sasaran manajemen risiko terkait keamanan siber Bank secara keseluruhan. Toleransi risiko terkait keamanan siber merupakan kemampuan Bank untuk menerima kejadian risiko terkait keamanan siber dan dampaknya. Toleransi risiko dimaksud merupakan penjabaran lebih lanjut dari tingkat risiko yang akan diambil terkait keamanan siber. Dalam menetapkan tingkat risiko yang akan diambil dan toleransi risiko terkait keamanan siber, Direksi harus memperhatikan strategi, tujuan, dan kemampuan Bank dalam mengambil risiko (*risk bearing capacity*).
		1.3. Budaya dan Kesadaran Risiko terkait Keamanan Siber	1.3.a. Direksi mengembangkan budaya mengenai tanggung jawab terkait keamanan siber bagi pegawai di semua level.	Budaya ini disampaikan melalui komunikasi yang jelas dan efektif serta mencakup informasi yang relevan tentang strategi keamanan siber kepada seluruh pegawai untuk memastikan terciptanya keamanan siber.
			1.3.b. Direksi membangun dan memelihara kesadaran dan komitmen yang kuat terhadap keamanan siber Bank.	Hal ini dapat dilakukan antara lain dengan program peningkatan kesadaran (*awareness*) terhadap keamanan siber yang dilakukan secara berkala dan berkelanjutan minimal setahun sekali, antara lain melalui seminar, diskusi, *workshop*, dan/atau diseminasi kebijakan dan prosedur keamanan siber. Program kesadaran dimaksud harus dikaji secara berkala dan dikinikan untuk memastikan substansi program sesuai dengan isu dan risiko dari ancaman siber yang relevan dan sedang berkembang.
			1.3.c. Bank memastikan efektivitas pemahaman dan penerapan kebijakan	Salah satu cara memverifikasi pemahaman dan kesadaran terhadap keamanan siber yaitu dengan melakukan simulasi *phishing* dengan cara

				keamanan siber bagi seluruh pegawai dan pemangku kepentingan terkait.	mengirimkan *email blast* kepada seluruh pegawai untuk mengukur respons terhadap *phishing* dan serangan surat elektronik *(email)* serupa setidaknya sekali setiap tahun.
2	Kerangka Manajemen Risiko terkait Keamanan Siber	2.1. Strategi Manajemen Risiko terkait Keamanan Siber	2.1.a.	Bank merumuskan strategi manajemen risiko terkait keamanan siber yang sepadan dengan kerentanan dan tingkat eksposur Bank terhadap ancaman siber serta sejalan dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber serta strategi bisnis secara keseluruhan.	Strategi manajemen risiko terkait keamanan siber disusun untuk memastikan bahwa eksposur risiko terkait keamanan siber Bank dikelola secara terkendali sesuai dengan kebijakan dan prosedur internal Bank serta peraturan perundang-undangan dan ketentuan lain. Dalam menyusun strategi manajemen risiko terkait keamanan siber, Bank mempertimbangkan paling sedikit: 1) kebutuhan keamanan siber Bank saat ini; 2) berorientasi jangka menengah dan jangka panjang untuk memastikan kelangsungan usaha Bank; dan 3) faktor lain, seperti hasil evaluasi pelaksanaan kebijakan keamanan siber, perkembangan teknologi dan ancaman atau modus serangan siber terkini, kecukupan SDM dan infrastruktur pendukung, karakteristik dan kompleksitas kegiatan usaha, serta kondisi keuangan Bank.
			2.1.b.	Bank memastikan kejelasan seluruh peran dan tanggung jawab terkait keamanan siber dalam strategi manajemen risiko terkait keamanan siber.	Strategi manajemen risiko terkait keamanan siber paling sedikit mencakup uraian atas hal-hal sebagai berikut: 1) pemahaman tentang risiko terkait keamanan siber secara keseluruhan dan kaitannya dengan bisnis Bank, tingkat eksposur terhadap risiko terkait keamanan siber, serta kondisi keamanan siber Bank saat ini;

				2) identifikasi, klasifikasi, dan penentuan prioritas fungsi kritis, aset TI, dan interkoneksi sistem (*interconnectivity*) untuk memperoleh pemahaman yang lengkap dan akurat tentang profil risiko terkait keamanan siber Bank; 3) identifikasi ancaman dan penanggulangan permasalahan keamanan siber, termasuk langkah yang diperlukan untuk menanggulangi risiko reputasi yang dapat merusak kepercayaan nasabah terhadap Bank; 4) kontrol keamanan untuk melindungi aset TI Bank terhadap ancaman siber yang berkembang; 5) deteksi insiden siber secara tepat waktu melalui pengawasan dan pemantauan secara berkala; dan 6) kebijakan dan prosedur penanganan insiden siber yang rinci untuk mendukung pemulihan yang cepat dan efektif dari dampak yang diakibatkan antara lain oleh insiden siber.
			2.1.c. Direksi mengomunikasikan strategi manajemen risiko terkait keamanan siber secara efektif kepada seluruh satuan kerja dan pegawai agar dipahami secara jelas.	
			2.1.d. Direksi melakukan kaji ulang strategi manajemen risiko terkait keamanan siber secara berkala untuk menentukan perlu atau	

			tidaknya dilakukan perubahan terhadap strategi manajemen risiko tersebut.	
		2.2. Kecukupan Perangkat Organisasi terkait Keamanan Siber	2.2.a. Direksi memastikan struktur organisasi Bank telah disertai dengan kejelasan tugas dan tanggung jawab mengenai penerapan manajemen risiko terkait keamanan siber pada seluruh satuan kerja yang disesuaikan dengan tujuan dan kebijakan usaha serta ukuran dan kompleksitas kegiatan usaha Bank.	
			2.2.b. Struktur organisasi dirancang untuk memastikan bahwa satuan kerja yang melakukan fungsi pengendalian intern terhadap manajemen risiko terkait keamanan siber memiliki independensi terhadap satuan kerja bisnis.	
			2.2.c. Bank memastikan satuan kerja manajemen risiko memiliki fungsi yang menangani penerapan	Wewenang dan tanggung jawab fungsi yang menangani penerapan manajemen risiko terkait keamanan siber, paling sedikit:

			manajemen risiko terkait keamanan siber.	1) memberikan masukan kepada Direksi dalam penyusunan kebijakan, strategi, dan kerangka manajemen risiko terkait keamanan siber; 2) mengembangkan prosedur dan alat untuk penerapan kontrol keamanan siber; 3) mendesain dan menerapkan perangkat yang dibutuhkan dalam penerapan kontrol keamanan siber; 4) memantau implementasi kebijakan, strategi, dan kerangka manajemen risiko terkait keamanan siber yang ditetapkan oleh Direksi dan telah disetujui oleh Dewan Komisaris; 5) melakukan pengujian guna mengetahui dampak dari implementasi kebijakan dan strategi manajemen risiko terkait keamanan siber terhadap profil risiko Bank secara keseluruhan; 6) mengkaji usulan produk baru dan penggunaan teknologi baru yang dikembangkan oleh suatu unit tertentu pada Bank yang difokuskan terutama pada dampak dari produk baru dan penggunaan teknologi baru tersebut terhadap eksposur risiko terkait keamanan siber Bank secara keseluruhan; dan 7) memberikan rekomendasi untuk penerapan manajemen risiko terkait keamanan siber kepada Direksi dan/atau satuan kerja lainnya.
			2.2.d. Bank memiliki unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber.	Struktur unit atau fungsi yang bertugas menangani ketahanan dan keamanan siber disesuaikan dengan ukuran dan kompleksitas kegiatan usaha Bank serta risiko terkait keamanan siber Bank.

		2.3. Kecukupan Kebijakan, Prosedur, dan Penetapan Limit Risiko terkait Keamanan Siber	2.3.a. Direksi menetapkan kebijakan dan prosedur yang dituangkan secara tertulis dalam menerapkan manajemen risiko terkait keamanan siber dan ketahanan siber.	Kebijakan dan prosedur tersebut harus sejalan dengan visi, misi, dan strategi bisnis Bank.
			2.3.b. Bank mendesain dan mengimplementasikan kebijakan dan prosedur dengan memperhatikan karakteristik dan kompleksitas kegiatan usaha, tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*), profil risiko, serta peraturan yang ditetapkan otoritas terkait dengan keamanan siber.	
			2.3.c. Bank melakukan internalisasi kebijakan manajemen risiko terkait keamanan siber, termasuk strategi dan tujuan manajemen risiko terkait keamanan siber, ke dalam proses bisnis pada seluruh lini bisnis dan aktivitas pendukung, termasuk kebijakan yang bersifat	

			spesifik sesuai dengan kebutuhan lini bisnis dan aktivitas pendukung Bank.	
			2.3.d. Bank menyusun kebijakan manajemen risiko terkait keamanan siber yang memadai.	Kebijakan manajemen risiko terkait keamanan siber disusun dengan menggunakan standar dan pedoman yang berlaku secara nasional maupun internasional sebagai bahan perbandingan, serta konsisten dengan kerangka manajemen risiko Bank secara keseluruhan. Kebijakan tersebut paling sedikit memuat: 1) cara Bank menetapkan toleransi risiko terkait keamanan siber dan tata cara Bank mengidentifikasi, mengurangi, dan mengelola risiko terkait keamanan siber; 2) rencana kelangsungan usaha (*business continuity plan*) atas kemungkinan kondisi ekstern dan intern terburuk dari serangan siber, antara lain melalui pelaksanaan *business impact analysis*; 3) hal yang spesifik terkait dengan keamanan siber, antara lain: a) kepatuhan SDM terhadap kebijakan manajemen risiko terkait keamanan siber termasuk sanksi yang dikenakan dalam hal terjadi pelanggaran; b) keamanan informasi termasuk pengaturan mengenai otentikasi antara lain melalui *single* ID yang unik dan pengaturan tenggat waktu kedaluwarsa hak akses akun pengguna, serta prosedur penambahan/perubahan/ penghapusan hak akses dalam hal terjadi perpindahan pegawai Bank;

				c) metode pelaporan dari pegawai Bank dan nasabah terkait kehilangan perangkat keras maupun perangkat lunak yang memungkinkan untuk digunakan sebagai sarana untuk melakukan serangan siber; d) metode manajemen data termasuk namun tidak terbatas pada pelindungan data, transfer data, dan penghapusan data; e) metode pengendalian kriptografi; f) kepatuhan terhadap ketentuan peraturan perundang-undangan mengenai hak kekayaan intelektual; g) metode verifikasi integritas serta pengujian terhadap perangkat keras dan perangkat lunak yang diperoleh dari luar Bank; dan h) metode verifikasi penerapan *secure coding* pada perangkat lunak yang dikembangkan oleh Bank untuk memastikan bahwa perangkat lunak tidak mengandung celah keamanan yang dilakukan melalui antara lain analisis statis dan analisis dinamis.
			2.3.e. Bank memiliki prosedur yang merupakan turunan dari kebijakan manajemen risiko terkait keamanan siber, yang dapat berupa pengendalian yang bersifat umum pada seluruh lini bisnis dan aktivitas pendukung Bank dan kontrol yang bersifat	

				spesifik pada masing-masing lini bisnis dan aktivitas pendukung Bank.	
			2.3.f.	Bank memiliki kebijakan dan prosedur keamanan siber yang digunakan untuk mengatur pelindungan aset TI.	Kebijakan dan prosedur keamanan siber paling sedikit mengatur tujuan, cakupan, fungsi, tanggung jawab, komitmen manajemen, dan koordinasi antar unit atau satuan kerja dalam organisasi Bank.
			2.3.g.	Bank memiliki kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga yang mengatur tentang pengelolaan data/informasi digital milik Bank (termasuk data nasabah yang dimiliki Bank) oleh pihak ketiga dan subkontraktor dari pihak ketiga.	Pengelolaan data dan informasi digital termasuk pemrosesan dan penghapusan atas data dan informasi. Kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga paling sedikit memuat: 1) proses untuk memblokir upaya akses perangkat milik karyawan serta perangkat milik pihak ketiga dan subkontraktor dari pihak ketiga yang tidak aman; 2) validasi dan dokumentasi atas implikasi keamanan dari semua perubahan dalam koneksi jaringan eksternal atau pihak ketiga dan subkontraktor dari pihak ketiga; 3) pengaturan akses pegawai pihak ketiga dan subkontraktor dari pihak ketiga ke data Bank yang sensitif atau kritikal dalam sistem yang di-*hosting* Bank serta pihak ketiga dan subkontraktor dari pihak ketiga dilacak secara aktif berdasarkan prinsip hak istimewa; 4) autentikasi yang kuat untuk mengamankan semua akses pihak ketiga dan subkontraktor dari pihak

				ketiga ke jaringan dan/atau sistem dan aplikasi Bank; 5) pemantauan dan pengujian kontrol untuk koneksi eksternal utama dan cadangan atau pihak ketiga dan subkontraktor dari pihak ketiga secara berkala; 6) kontrol keamanan yang dirancang dan diverifikasi untuk mendeteksi dan mencegah intrusi dari koneksi eksternal atau pihak ketiga dan subkontraktor dari pihak ketiga; 7) kejelasan tanggung jawab untuk menanggapi insiden siber serta pemberitahuan atas insiden dan kerentanan keamanan siber oleh pihak ketiga dan subkontraktor dari pihak ketiga yang terhubung ke jaringan atau memiliki akses terhadap data sensitif atau kritikal Bank; 8) identifikasi dan dokumentasi yang jelas terhadap aliran data, jaringan, serta sistem dari koneksi eksternal dan pihak ketiga serta subkontraktor dari pihak ketiga yang terhubung ke jaringan Bank; dan 9) terdapat proses pembaruan diagram aliran data, jaringan, serta sistem dari koneksi eksternal dan pihak ketiga serta subkontraktor dari pihak ketiga yang terhubung ke jaringan Bank dalam hal terjadi perubahan dan ditinjau secara periodik.
			2.3.h. Bank menerapkan manajemen risiko terkait keamanan siber untuk pihak ketiga dan	

				subkontraktor dari pihak ketiga.	
			2.3.i.	Bank menetapkan standar minimum kendali keamanan siber bagi pihak ketiga dan subkontraktor dari pihak ketiga, yaitu: 1) ketentuan kerahasiaan di kontrak kerja sama; 2) ketersediaan tata kelola pengamanan siber di pihak ketiga dan subkontraktor dari pihak ketiga (kebijakan, prosedur, ketentuan, dan lainnya); dan 3) pengelolaan risiko terkait keamanan siber termasuk manajemen insiden siber di pihak ketiga dan subkontraktor dari pihak ketiga.	
			2.3.j.	Bank memiliki limit risiko terkait keamanan siber yang sesuai dengan tingkat risiko yang akan diambil (*risk appetite*), toleransi risiko (*risk tolerance*), dan strategi	Dalam rangka pengendalian risiko terkait keamanan siber, limit digunakan sebagai ambang batas untuk menentukan tingkat intensitas mitigasi risiko terkait keamanan siber yang akan dilaksanakan oleh manajemen.

				Bank terkait keamanan siber secara keseluruhan serta dengan memperhatikan kemampuan Bank untuk dapat menyerap eksposur risiko terkait keamanan siber atau kerugian yang timbul, pengalaman kerugian di masa lalu, kemampuan SDM, dan kepatuhan terhadap ketentuan eksternal yang berlaku.	
			2.3.k.	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber harus didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.	
			2.3.l.	Direksi melakukan kaji ulang atas kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber secara berkala untuk menyesuaikan dengan kondisi terkini.	

3	Proses Manajemen Risiko, Kecukupan SDM, dan Kecukupan Sistem Informasi Manajemen Risiko, terkait Keamanan Siber	3.1. Proses Manajemen Risiko terkait Keamanan Siber (Identifikasi, Pengukuran, Pemantauan, dan Pengendalian)	3.1.a. Bank melaksanakan identifikasi seluruh risiko terkait keamanan siber secara berkala.	Proses identifikasi risiko terkait keamanan siber dilakukan dengan menganalisis seluruh sumber risiko terkait keamanan siber. Sumber risiko tersebut dapat berasal dari SDM, proses, sistem, maupun faktor ekstern Bank, dengan penjelasan sebagai berikut: 1) SDM SDM merupakan sumber dari risiko terkait keamanan siber dalam bentuk ketidakmampuan SDM dalam melaksanakan tugas terkait pengamanan aset TI Bank atau faktor kurangnya *security awareness* SDM dalam melaksanakan tugas dan proses kerja sehari-hari, serta faktor lain terkait dengan integritas SDM Bank. 2) Proses Desain dan implementasi proses bisnis dalam Bank dapat menyebabkan terjadinya insiden siber bagi Bank. Kelemahan dalam proses tersebut antara lain tidak adanya proses *secure channel* saat transmisi, audit aspek keamanan tidak dilaksanakan secara berkala, manajemen kata sandi yang buruk, dan penggunaan akses internet publik yang tidak aman. 3) Sistem Kelemahan pada TI dan infrastruktur Bank dapat menjadi sumber risiko terkait keamanan siber. Kurangnya pengujian pengamanan, kontrol, dan *monitoring* ancaman dan kerentanan, kelemahan sistem (seperti tidak tersedianya *anti-malware*/antivirus), dan sistem yang tidak *update,* menjadi jalan bagi masuknya risiko terkait keamanan siber kepada Bank.

				4) Faktor Ekstern Faktor ekstern yang menjadi penyebab utama risiko terkait keamanan siber bagi Bank yaitu kurangnya *security awareness* dari nasabah. Selain itu, semakin berkembangnya taktik dan kecanggihan pelaku serangan siber juga menjadi faktor ekstern yang mengakibatkan munculnya risiko terkait keamanan siber.
			3.1.b. Bank memastikan tersedianya metode atau sistem untuk melakukan identifikasi risiko pada seluruh kegiatan Bank yang terkait dengan keamanan siber.	
			3.1.c. Bank melakukan pengukuran risiko secara berkala untuk seluruh kegiatan Bank yang terkait dengan keamanan siber.	
			3.1.d. Bank memiliki sistem pengukuran risiko untuk mengukur eksposur risiko terkait keamanan siber pada Bank sebagai acuan untuk melakukan pengendalian.	Sistem tersebut paling sedikit dapat mengukur: 1) sensitivitas kegiatan Bank yang terkait dengan keamanan siber terhadap perubahan faktor yang memengaruhinya, baik dalam kondisi normal maupun tidak normal; 2) kecenderungan perubahan faktor dimaksud berdasarkan fluktuasi yang terjadi pada masa lalu dan korelasinya; 3) faktor risiko terkait keamanan siber; 4) eksposur risiko terkait keamanan siber; dan

				5) seluruh risiko yang melekat pada kegiatan Bank terkait keamanan siber. Metode pengukuran risiko terkait keamanan siber dapat dilakukan secara kuantitatif dan/atau kualitatif. Pemilihan metode pengukuran disesuaikan dengan karakteristik dan kompleksitas kegiatan usaha Bank.
			3.1.e. Bank melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber secara berkala atau sewaktu-waktu dalam hal diperlukan untuk memastikan kesesuaian asumsi, akurasi, kewajaran dan integritas data, serta prosedur yang digunakan untuk mengukur risiko terkait keamanan siber.	
			3.1.f. Bank memiliki sistem dan prosedur pemantauan risiko terkait keamanan siber yang antara lain mencakup pemantauan risiko terkait keamanan siber terhadap besarnya eksposur risiko, toleransi risiko (*risk tolerance*), kepatuhan limit intern, dan hasil *stress test*	Pemantauan dilakukan baik oleh unit bisnis maupun oleh satuan kerja manajemen risiko. Hasil pemantauan disajikan dalam laporan berkala yang disampaikan kepada pihak manajemen Bank dalam rangka mitigasi risiko terkait keamanan siber dan penentuan tindakan yang diperlukan.

				maupun konsistensi pelaksanaan dengan kebijakan dan prosedur yang ditetapkan.	
			3.1.g.	Bank menyiapkan suatu sistem dan prosedur *back-up* yang efektif untuk mencegah terjadinya gangguan dalam proses pemantauan risiko terkait keamanan siber dan melakukan pengecekan serta penilaian kembali secara berkala terhadap sistem *back-up* tersebut.	
			3.1.h.	Bank memiliki sistem pengendalian risiko terkait keamanan siber yang memadai dengan mengacu pada kebijakan dan prosedur yang telah ditetapkan.	Proses pengendalian risiko terkait keamanan siber yang diterapkan Bank harus disesuaikan dengan eksposur risiko maupun tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*). Pengendalian risiko terkait keamanan siber dapat dilakukan oleh Bank, antara lain penyediaan sistem *back-up* dan penyelenggaraan rencana pemulihan bencana (*Disaster Recovery Plan*/DRP).
		3.2. Kecukupan SDM terkait Keamanan Siber	3.2.a.	Direksi memastikan kecukupan kuantitas dan kualitas SDM yang ada di Bank dan memastikan SDM dimaksud memahami tugas dan tanggung jawabnya dalam pelaksanaan manajemen	

				risiko terkait keamanan siber, baik untuk unit bisnis, satuan kerja manajemen risiko, maupun unit pendukung yang bertanggung jawab atas pelaksanaan manajemen risiko terkait keamanan siber.	
			3.2.b.	Direksi mengembangkan sistem penerimaan, pengembangan, dan pelatihan pegawai, termasuk rencana suksesi manajerial serta remunerasi yang memadai untuk memastikan tersedianya pegawai yang kompeten di bidang manajemen risiko terkait keamanan siber.	
			3.2.c.	Direksi memastikan bahwa seluruh SDM memiliki pemahaman yang memadai atas risiko terkait keamanan siber dan mampu mengomunikasikan implikasi risiko terkait keamanan siber kepada	

				Direksi, Dewan Komisaris, manajemen, dan nasabah.	
			3.2.d.	Direksi memastikan agar seluruh SDM memahami strategi, tingkat risiko terkait keamanan siber yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber, kerangka manajemen risiko terkait keamanan siber yang telah ditetapkan oleh Direksi dan disetujui oleh Dewan Komisaris, serta memastikan seluruh SDM menerapkannya secara konsisten dalam aktivitas yang ditangani.	
			3.2.e.	Bank memiliki informasi yang utuh mengenai seluruh pegawai Bank, yang meliputi pengetahuan, keterampilan, kemampuan, dan karakter dari pegawai.	Hal yang dapat dilakukan oleh Bank salah satunya dengan melakukan pemeriksaan latar belakang (*background check*) untuk pegawai baru, dalam rangka melindungi pemangku kepentingan maupun reputasi Bank, serta mencegah potensi terjadinya *fraud*.
			3.2.f.	Bank mengembangkan dan mengimplementasikan program berkelanjutan	Program peningkatan kapasitas dapat berupa pelatihan terkait: 1) identifikasi ancaman siber saat ini termasuk berbagai bentuk serangan *social engineering*,

				untuk peningkatan kapasitas terkait keamanan siber kepada seluruh pegawai yang relevan, termasuk level Direksi, Dewan Komisaris, dan manajemen untuk memastikan bahwa setiap pegawai memiliki kompetensi dan keahlian untuk menjalankan peran dan tanggung jawab secara efektif.	antara lain *phishing*, *scam phone*, dan *impersonation call*; 2) taktik serangan siber; 3) pengamanan termasuk penggunaan *secure authentication* serta cara mengidentifikasi, melindungi, menyimpan, mengirimkan, mengarsipkan, dan memusnahkan informasi sensitif dengan benar; 4) penyebab kebocoran data secara tidak sengaja, seperti kehilangan perangkat seluler pegawai atau ketidaksengajaan mengirim surat elektronik ke orang yang salah; 5) pelindungan data, pembatasan penggunaan, dan dokumentasi proses penanganan data sensitif pemangku kepentingan; 6) kewajiban menjaga data pribadi dan pengungkapan data pribadi sesuai dengan ketentuan peraturan perundang-undangan; 7) penerapan *secure coding* yang baik dalam pengembangan perangkat lunak; dan/atau 8) praktik penanggulangan dan pemulihan insiden siber yang tepat. Adapun frekuensi dan substansi peningkatan kapasitas disesuaikan dengan peran dan tanggung jawab setiap pegawai.
			3.2.g.	Bank melakukan analisis kesenjangan (*gap analysis*) untuk memahami tingkat pengetahuan dan kemampuan pegawai terkait keamanan siber	Dalam melakukan peningkatan kapasitas pegawai, Bank dapat mengacu pada ketentuan peraturan perundang-undangan mengenai pelindungan infrastruktur informasi vital beserta ketentuan turunannya yang terkait.

			dan menggunakan informasi tersebut untuk membuat rencana aksi peningkatan kapasitas pegawai.	Contoh peningkatan kapasitas pegawai antara lain pendidikan dan pelatihan terkait keamanan siber secara berkala.
		3.3. Kecukupan Sistem Informasi Manajemen Risiko terkait Keamanan Siber	3.3.a. Bank memiliki sistem informasi manajemen risiko terkait keamanan siber dan mengembangkannya sesuai dengan kebutuhan Bank dalam rangka penerapan manajemen risiko terkait keamanan siber yang efektif.	Sebagai bagian dari proses manajemen risiko, sistem informasi manajemen risiko terkait keamanan siber Bank digunakan untuk mendukung pelaksanaan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko terkait keamanan siber. Sistem informasi manajemen risiko terkait keamanan siber dapat memastikan paling sedikit: 1) tersedianya informasi yang akurat, lengkap, informatif, tepat waktu, dan dapat diandalkan agar dapat digunakan Direksi, Dewan Komisaris, dan fungsi yang terkait dalam penerapan manajemen risiko terkait keamanan siber untuk menilai, memantau, dan memitigasi risiko terkait keamanan siber yang dihadapi Bank dan/atau dalam rangka proses pengambilan keputusan oleh Direksi; 2) efektivitas penerapan manajemen risiko terkait keamanan siber mencakup kebijakan dan prosedur manajemen risiko terkait keamanan siber serta penetapan limit risiko terkait keamanan siber; dan 3) tersedianya informasi tentang hasil atau realisasi penerapan manajemen risiko terkait keamanan siber dibandingkan dengan target yang ditetapkan oleh Bank sesuai dengan kebijakan dan strategi penerapan manajemen risiko terkait keamanan siber.

			3.3.b. Bank memastikan sistem informasi manajemen risiko terkait keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha Bank serta adaptif terhadap perubahan.	
			3.3.c. Bank melakukan kaji ulang secara berkala atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko terkait keamanan siber untuk memastikan bahwa cakupan informasi tersebut telah memadai sesuai perkembangan tingkat kompleksitas kegiatan usaha Bank.	
			3.3.d. Sebagai bagian dari sistem informasi manajemen risiko terkait keamanan siber, laporan tingkat maturitas keamanan siber disusun secara berkala oleh unit atau fungsi yang bertugas menangani ketahanan dan keamanan	

				siber Bank. Frekuensi penyampaian laporan tingkat maturitas keamanan siber kepada Direksi terkait dan komite manajemen risiko harus ditingkatkan sesuai kebutuhan terutama dalam hal terdapat perkembangan serangan dan ancaman siber yang berubah dengan cepat.	
			3.3.e.	Bank memastikan sistem informasi manajemen risiko terkait keamanan siber mendukung pelaksanaan pelaporan tingkat maturitas keamanan siber kepada Otoritas Jasa Keuangan.	
4.	Sistem Pengendalian Risiko terkait Keamanan Siber	4.1. Kecukupan Sistem Pengendalian Intern	4.1.a.	Bank melaksanakan sistem pengendalian intern secara efektif dalam penerapan manajemen risiko terkait keamanan siber dengan mengacu pada kebijakan dan prosedur yang telah ditetapkan.	Dalam melaksanakan sistem pengendalian intern, Bank memastikan penerapan prinsip pemisahan fungsi (*four eyes principle*) telah memadai dan dilaksanakan secara konsisten. Sistem pengendalian intern menjadi tanggung jawab seluruh satuan kerja bisnis dan satuan kerja pendukung termasuk satuan kerja kepatuhan, satuan kerja manajemen risiko, dan satuan kerja audit intern. Dalam menerapkan sistem pengendalian intern, Bank memperhatikan paling sedikit:

				1) penerapan manajemen risiko terkait keamanan siber telah mencapai hasil yang diharapkan; 2) kesesuaian antara sistem pengendalian intern dengan tingkat risiko inheren dan penerapan manajemen risiko terkait keamanan siber pada Bank; 3) penetapan wewenang dan tanggung jawab untuk pemantauan kepatuhan kebijakan dan prosedur manajemen risiko terkait keamanan siber serta penetapan limit risiko terkait keamanan siber; 4) penetapan jalur pelaporan dan pemisahan fungsi yang jelas dari satuan kerja bisnis (*risk-taking unit*) kepada satuan kerja yang melaksanakan fungsi pengendalian risiko terkait keamanan siber; 5) struktur organisasi yang menggambarkan secara jelas tugas dan tanggung jawab masing-masing unit dan individu; 6) pelaporan penerapan manajemen risiko terkait keamanan siber termasuk penanggulangan dan pemulihan insiden siber yang akurat dan tepat waktu; 7) kecukupan prosedur untuk memastikan kepatuhan Bank terhadap ketentuan peraturan perundang-undangan; 8) kaji ulang yang efektif, independen, dan obyektif terhadap kebijakan, kerangka, dan prosedur manajemen risiko terkait keamanan siber Bank; 9) pengujian dan kaji ulang yang memadai terhadap sistem informasi manajemen risiko terkait keamanan siber;

				10) dokumentasi secara lengkap dan memadai terhadap cakupan, prosedur operasional, temuan audit, tanggapan berdasarkan hasil audit terhadap keamanan siber, serta tindak lanjut hasil audit; dan 11) verifikasi dan kaji ulang secara berkala dan berkesinambungan terhadap penanganan kelemahan Bank yang bersifat material serta tindakan untuk memperbaiki penyimpangan yang terjadi terhadap keamanan siber.
			4.1.b. Bank melaksanakan sistem pengendalian intern secara efektif dalam penerapan proses ketahanan siber dengan mengacu pada kebijakan dan prosedur yang telah ditetapkan.	Dalam melaksanakan sistem pengendalian intern secara efektif, Bank memperhatikan paling sedikit: 1) seluruh tanggung jawab keamanan siber dan keamanan informasi telah ditentukan, dialokasikan, serta terkoordinasi dengan baik; 2) kepatuhan atas kewajiban semua SDM termasuk pihak ketiga untuk menerapkan keamanan siber sesuai dengan kebijakan dan prosedur yang telah ditetapkan; 3) kecukupan persyaratan keamanan siber terkait akses *supplier* terhadap aset TI Bank yang telah didokumentasikan dengan baik; 4) kecukupan pengujian terhadap keberadaan informasi yang dapat berguna bagi penyerang seperti *network diagram*, *file* konfigurasi, laporan *penetration test*, surat elektronik, atau dokumen yang berisikan kata sandi atau informasi lain yang penting untuk sistem operasi (*operating system*); 5) kecukupan penetapan program untuk identifikasi kerentanan atau *penetration test* secara berkala

				terhadap aplikasi berbasis web, aplikasi *client-based*, aplikasi *mobile*, *wireless*, *server*, dan perangkat jaringan; 6) kecukupan kualitas dan kuantitas SDM, cakupan tugas serta tanggung jawab *red-team* (*offensive security professionals* yang melakukan penyerangan atas sistem) dan *blue-team* (*defensive security professionals* yang melakukan pertahanan atas sistem) serta pengujian secara berkala yang dilakukan dalam rangka mengukur kesiapan Bank untuk mengidentifikasi dan menghentikan serangan atau merespons dengan cepat dan efektif dari insiden siber yang terjadi; 7) pemisahan lingkungan antara sistem produksi dengan pengembangan serta prosedur izin akses kepada pengembangan tanpa adanya pengawasan dari bagian keamanan siber Bank; 8) penggunaan standar *hardening configuration template* dalam hal Bank mengandalkan *database* dan pengujian pada semua sistem perangkat lunak yang menjadi bagian penting dari proses bisnis Bank; 9) pelindungan aplikasi web Bank dengan menggunakan *firewall* aplikasi berbasis web (WAFs) serta memastikan bahwa pelindungan tersebut berjalan di semua perangkat komputasi; 10) pelindungan alamat IP internal Bank dengan menggunakan *Network Address Translation* (NAT); 11) penggunaan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS);

				12) penggunaan antivirus dan anti-*malware* yang dilakukan secara terpusat dan selalu dikinikan terhadap perangkat *endpoint*; 13) penggunaan *Data Loss Prevention* (DLP) atau *Network Access Control* (NAC); 14) pelaksanaan *risk assessment* terhadap risiko terkait keamanan siber secara berkala; 15) pencegahan atau pengurangan terhadap dampak yang tidak diinginkan dari risiko terkait keamanan siber; 16) penerapan pengendalian keamanan (*security control*) untuk meminimalisasi risiko; 17) ketersediaan dan kecukupan inventaris risiko (*risk register*) terkait keamanan siber yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria Bank, antara lain atas seluruh aplikasi yang memproses data pemangku kepentingan Bank; 18) penerapan *continual improvement* terhadap keamanan siber; 19) implementasi kebijakan *Domain-based Message Authentication and Conformance* (DMARC) atau protokol autentikasi surat elektronik untuk melindungi domain dari penggunaan yang tidak sah agar tidak digunakan dalam serangan atau aktivitas ancaman keamanan siber antara lain penyusupan surat elektronik bisnis (*business email intrusion*) dan *phishing* melalui surat elektronik (*email phishing*); 20) melakukan filter terhadap seluruh jenis *file* lampiran surat elektronik;

				21) penerapan metode *email sandboxing* terhadap seluruh lampiran surat elektronik untuk mencegah dan analisis keamanan lebih lanjut terhadap *malicious behavior*; dan 22) integrasi keamanan siber dalam seluruh fase perencanaan dan pengembangan seluruh proyek TI.
			4.1.c. Satuan kerja audit intern melakukan pemantauan terhadap perbaikan hasil temuan. Temuan yang belum ditindaklanjuti harus dilaporkan kepada Direksi dan/atau Dewan Komisaris untuk diambil langkah yang diperlukan.	
			4.1.d. Bank memiliki sistem rotasi rutin untuk menghindari potensi *self-dealing*, persekongkolan atau penyembunyian suatu dokumentasi atau aktivitas yang tidak wajar.	
		4.2. Kecukupan Kaji Ulang	4.2.a. Bank melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara berkala sesuai dengan karakteristik dan kompleksitas Bank.	Kaji ulang dan evaluasi tersebut dilakukan oleh satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber dan satuan kerja audit intern.

			4.2.b. Bank memastikan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber melakukan kaji ulang dan evaluasi secara memadai.	Penerapan kaji ulang dan evaluasi oleh satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber paling sedikit terhadap: 1) kesesuaian kerangka manajemen risiko terkait keamanan siber, yang mencakup kebijakan, struktur organisasi, alokasi sumber daya, desain proses manajemen risiko terkait keamanan siber, sistem informasi, pelaporan risiko terkait keamanan siber Bank, dan pelaksanaan manajemen risiko terkait keamanan siber; 2) metode, asumsi, dan variabel yang digunakan untuk mengukur risiko terkait keamanan siber dan limit eksposur risiko terkait keamanan siber; 3) perbandingan antara hasil dari metode pengukuran risiko terkait keamanan siber yang menggunakan simulasi atau proyeksi ke depan dengan hasil aktual; 4) perbandingan antara asumsi yang digunakan dalam metode pengukuran risiko dengan kondisi aktual; 5) perbandingan antara limit risiko terkait keamanan siber yang ditetapkan dengan eksposur risiko terkait keamanan siber yang aktual; dan 6) penerapan manajemen risiko terkait keamanan siber oleh satuan kerja bisnis atau satuan kerja pendukung.
			4.2.c. Bank memastikan satuan kerja audit intern melakukan kaji ulang dan evaluasi secara memadai.	Penerapan kaji ulang dan evaluasi oleh satuan kerja audit intern paling sedikit terhadap: 1) keandalan kerangka manajemen risiko terkait keamanan siber, yang mencakup kebijakan, struktur organisasi, alokasi sumber daya, desain

				proses manajemen risiko terkait keamanan siber, sistem informasi, dan pelaporan risiko terkait keamanan siber Bank; 2) penerapan manajemen risiko terkait keamanan siber oleh seluruh pegawai, termasuk kaji ulang terhadap pelaksanaan pemantauan oleh satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber; 3) penerapan manajemen data termasuk pelindungan; 4) penggunaan algoritma enkripsi dalam pengembangan perangkat lunak; 5) penggunaan *tool* identifikasi kerentanan secara mandiri, kemudian hasil identifikasi kerentanan digunakan sebagai titik awal dalam melakukan *penetration test*; 6) penggunaan akun khusus selain akun admin untuk melakukan *penetration test*; 7) pengendalian dan pemantauan atas akun pengguna atau sistem yang digunakan dalam melakukan *penetration test* untuk memastikan bahwa akun tersebut hanya digunakan untuk tujuan yang sah dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan; 8) penerapan keamanan informasi; 9) pelaksanaan secara berkala *security risk assessment* dan *security risk treatment*; 10) izin akses dari pengguna secara berkala (contoh: setiap 3 (tiga) bulan);

				11) dokumentasi/diagram yang menggambarkan seluruh aliran data di seluruh sistem dan jaringan termasuk pembaruannya; dan 12) penerapan dan dokumentasi standar konfigurasi (*port, protocol, service*) untuk semua sistem, seperti *operating system* dan aplikasi.
			4.2.d. Bank memastikan pihak yang melakukan kaji ulang dan evaluasi atas penerapan manajemen risiko terkait keamanan siber memiliki independensi dan kompetensi yang baik serta metode kaji ulang yang andal.	
			4.2.e. Bank memastikan bahwa hasil kaji ulang dan evaluasi atas penerapan manajemen risiko terkait keamanan siber telah disampaikan kepada Direksi dan Dewan Komisaris untuk diambil langkah perbaikan dan/atau penyempurnaan manajemen risiko terkait keamanan siber.	

I.c. Penilaian Kualitas Penerapan Proses Ketahanan Siber

Matriks Kontrol Penerapan Proses Ketahanan Siber

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
1.	Proses Identifikasi Aset, Ancaman, dan Kerentanan	1.a. Bank menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta pencatatan konfigurasi secara efektif.	Dalam melakukan manajemen aset TI, Bank paling sedikit: 1) melakukan inventarisasi aset TI antara lain perangkat keras, perangkat lunak, data, jaringan, dan infrastruktur untuk menetapkan prioritas aset TI berdasarkan klasifikasi kritikalitas dan sensitivitasnya, serta memastikan aset TI yang ada telah sesuai dengan kebutuhan Bank; 2) melakukan analisis, penilaian, dan klasifikasi atas aset TI untuk memperoleh informasi mengenai tingkat kritikalitas dan sensitivitas aset TI terhadap Bank dengan mempertimbangkan antara lain hasil *business impact analysis* Bank; 3) memiliki mekanisme pencatatan konfigurasi perangkat keras dan perangkat lunak secara efektif. Hal ini dapat dilakukan antara lain dengan menggunakan *system configuration management*; dan 4) melakukan inventarisasi aset TI secara berkala.
		1.b. Bank melakukan identifikasi kerentanan dan pemantauan terhadap perkembangan siber terkini untuk mengidentifikasi ancaman siber.	Dalam melakukan identifikasi kerentanan dan pemantauan terhadap perkembangan siber, Bank paling sedikit: 1) melakukan pemantauan seluruh sistem secara berkala untuk mengidentifikasi kerentanan. Frekuensi pelaksanaan identifikasi kerentanan dan pemantauan terhadap perkembangan siber yang terkini ditetapkan sesuai dengan tingkat kritikalitas sistem dan risiko yang dihadapi; 2) melakukan pemantauan terhadap perkembangan siber yang terkini, baik dari sisi teknologi, taktik dan teknik

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			serangan, serta prosedur atau pola serangan, untuk mengidentifikasi ancaman siber; 3) melakukan analisis atas ancaman dan kerentanan serta melakukan klasifikasi ancaman dan kerentanan berdasarkan potensi dampak yang ditimbulkan; dan 4) menyusun dan memelihara inventaris risiko (*risk register*).
		1.c. Bank melakukan pengujian keamanan siber secara berkala.	Dalam melakukan pengujian keamanan siber, Bank paling sedikit melakukan: 1) pengujian keamanan siber berdasarkan analisis kerentanan; 2) pengujian keamanan siber berdasarkan skenario; dan 3) upaya secara proaktif untuk menyusun skenario pengujian yang realistis, antara lain melalui *threat hunting* yang menyeluruh.
2.	Proses Pelindungan Aset	2.a. Bank menerapkan pengendalian keamanan (*security control*) yang komprehensif sesuai dengan hasil identifikasi aset, ancaman, dan kerentanan.	Pengendalian keamanan yang komprehensif bertujuan untuk memastikan: 1) kerahasiaan, integritas, dan ketersediaan dari data, informasi, serta sistem informasi; dan 2) kesesuaian dengan ketentuan peraturan perundang-undangan dan standar yang berlaku.
		2.b. Bank melakukan pemeliharaan dan perbaikan terhadap pengendalian keamanan atas aset TI sesuai dengan kebijakan dan prosedur yang berlaku.	
		2.c. Bank menerapkan sistem pengamanan yang dikelola	

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		dengan baik sesuai kebijakan dan prosedur yang berlaku.	
		2.d. Bank melakukan penginian pengendalian keamanannya secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan sesuai dengan hasil terkini dari proses identifikasi.	Peninjauan atas pengendalian keamanan siber yang diterapkan pada Bank dilakukan sesuai dengan kritikalitas aset TI berdasarkan identifikasi terkini.
		2.e. Bank menerapkan manajemen keamanan data dan informasi serta memastikan bahwa data dan/atau informasi dikelola sesuai dengan strategi manajemen risiko terkait keamanan siber pada organisasi untuk melindungi kerahasiaan, integritas, serta ketersediaan data dan informasi.	Dalam menerapkan manajemen keamanan data dan informasi, Bank paling sedikit melakukan: 1) pengelolaan data dan informasi yang memadai, antara lain terkait dengan pemindahan data, transfer data, dan pemusnahan data; 2) pelindungan data dan informasi pada saat disimpan, digunakan, maupun dikirim; 3) pengecekan integritas untuk verifikasi atas integritas perangkat lunak, *firmware*, perangkat keras serta data dan informasi; 4) pelindungan terhadap ketersediaan data dan informasi, dengan memperhatikan kepemilikan, periode retensi, serta penggunaan data dan informasi; 5) pemisahan antara lingkungan pengembangan dan pengujian dari lingkungan produksi; 6) proses *back-up* data yang dilakukan sesuai dengan kebutuhan bisnis dari hasil *business impact analysis* dan proses penyimpanan data *back-up* dilakukan secara memadai; 7) pengamanan, dokumentasi, serta pemantauan atas penggunaan data dan/atau informasi, dalam hal

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			terdapat kebutuhan untuk menerima atau menyampaikan data dan/atau informasi dari atau kepada pihak ketiga; dan 8) penerapan metode otomatis untuk sinkronisasi waktu atas *critical system clocks* dengan menggunakan protokol seperti *network time protocol*.
		2.f. Bank menerapkan manajemen pelindungan terhadap jaringan, perangkat keras, dan perangkat lunak.	Dalam menerapkan manajemen pelindungan, Bank paling sedikit: 1) memiliki perangkat pelindungan jaringan perimeter (misalnya *border router* dan *firewall*) yang memadai dan diverifikasi secara berkala, termasuk *implicit deny rule* atau *explicit deny rule*; 2) memiliki IPS untuk mencegah percobaan serangan siber; 3) implementasi pembatasan terhadap *inbound* dan *outbound network traffic* dalam jaringan untuk mencegah *malware*; 4) menggunakan *next generation endpoint protection* untuk membatasi aplikasi yang diunduh, diinstal, dan digunakan; 5) melakukan pemantauan terhadap *port* jaringan secara berkala; 6) menggunakan autentikasi terpusat untuk seluruh perangkat jaringan; 7) memastikan dilakukannya proses enkripsi untuk autentikasi dan transmisi data melalui jaringan nirkabel dan perangkat *mobile*, serta media penyimpanan ekstern;

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			8) memiliki perangkat keamanan jaringan, misalnya *Domain Name System* (DNS) *filtering service* atau DNS *security extensions*; 9) memiliki sistem pengecekan otomatis terhadap *spam/phishing/malware* pada surat elektronik termasuk yang ada dalam *cloud*; 10) menggunakan pembatasan penggunaan *scripting tools*; 11) memastikan seluruh jaringan, aplikasi, dan perangkat TI Bank masih mendapatkan *update support*, antara lain mencakup web *browser*, *email client*, sistem operasi (*operating system*), *database server*, perangkat jaringan, perangkat keamanan, serta memastikan *update support* tersebut segera dilakukan dalam hal terdapat *security patches*; 12) menggunakan *add-on* dan *plug-in* aplikasi sesuai dengan ketentuan organisasi; 13) memastikan: a) kecukupan proses formal pengelolaan konfigurasi *router*, *switch* dan *firewall*, meliputi perubahan dan pengujian seluruh perubahan konfigurasi *router*, *switch*, dan *firewall*; b) dokumentasi konfigurasi dan reviu berkala atas konfigurasi *router* dan *switch* minimal setiap 6 (enam) bulan; c) sinkronisasi *switch* dan *router startup configuration* dengan *running configuration*; d) kebijakan akun *default* konfigurasi, serta *back-up* atas konfigurasi perangkat tersebut; 14) mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan;

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			15) membatasi penggunaan aset untuk kepentingan pribadi dan penggunaan aset pihak ketiga pada jaringan Bank; 16) menetapkan hak akses administrator pada perangkat Bank untuk pegawai; 17) menonaktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh Bank (contoh: *port* USB, DVD, dan akses perangkat seluler); dan 18) menerapkan *whitelist* aplikasi untuk memastikan bahwa hanya *authorized software library* dan *signed script* yang dapat dijalankan oleh sistem.
		2.g. Bank menerapkan manajemen pelindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastruktur jaringan, dan komponen sistem yang dikelola oleh Bank.	Dalam menerapkan manajemen pelindungan terhadap akses dan pengguna, Bank paling sedikit: 1) mengimplementasikan identifikasi dan autentikasi pengelolaan akses terhadap seluruh perangkat lunak dan perangkat keras; 2) melakukan kendali terhadap akses pengguna, termasuk kompleksitas kata sandi, pembatasan percobaan dan penggunaan kembali kata sandi, serta permintaan kata sandi setelah perangkat tidak aktif untuk beberapa saat; 3) menerapkan pengamanan *endpoint* antara lain dengan menggunakan web URL *filtering*, *device control*, dan aplikasi kontrol pada seluruh perangkat *endpoint* pengguna termasuk *endpoint* yang terhubung ke *Virtual Private Network* (VPN); 4) menggunakan verifikasi *One Time Password* (OTP) untuk transaksi yang berisiko tinggi; 5) menerapkan IP *reputation* untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi;

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6) memastikan batasan akses pada *database*, misalnya menerapkan akses *read-only* bagi pengguna selain admin *database*; 7) menggunakan *Multi-Factor Authentication* (MFA) untuk akses data sensitif atau akses terhadap seluruh jaringan apabila diperlukan; 8) menonaktifkan komunikasi antar *workstation* untuk mencegah terjadinya serangan siber dan *disabled peer to peer* pada *wireless client* di perangkat; 9) memastikan seluruh pegawai menggunakan fitur *wireless* hanya untuk kepentingan Bank; 10) menonaktifkan fitur *auto-run content* terhadap perangkat yang terhubung ke sistem atau perangkat di Bank; dan 11) menerapkan metode autentikasi melalui saluran terenkripsi, baik untuk *login* ke jaringan maupun aplikasi.
		2.h. Bank menerapkan pelindungan yang memadai dalam pelaksanaan kerja sama antara Bank dengan pihak penyedia jasa TI, termasuk dalam penggunaan *cloud*.	Dalam menerapkan pelindungan yang memadai terkait pelaksanaan kerja sama antara Bank dengan pihak penyedia jasa TI, Bank paling sedikit: 1) memastikan telah terdapat pengendalian yang memadai untuk *logical access* ke sistem Bank; 2) menerapkan kebijakan klasifikasi kritikalitas dan sensitivitas terhadap data dan informasi yang disimpan pada *cloud*; 3) memastikan pengamanan yang menjadi tanggung jawab Bank telah dikonfigurasikan sesuai standar dan *best practices*;

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			4) memastikan kapabilitas SDM Bank untuk dapat melakukan konfigurasi sistem dan menerapkan kontrol pengamanan di *cloud*; 5) menggunakan *authorized cloud storage*; 6) memastikan otorisasi *traffic* pada layanan *cloud* hanya untuk kebutuhan bisnis dan operasional Bank; 7) membatasi akses *traffic cloud* hanya untuk alamat IP yang dikenal oleh Bank; 8) memastikan penyedia *cloud* telah menerapkan MFA; 9) memastikan penyedia *cloud* memiliki *data recovery center* yang terpisah secara geografis dan memiliki *recovery point objective* dan *recovery time objective* yang terdokumentasi; dan 10) memastikan penerapan *single-sign on* serta aksesnya melalui *Secure Socket Layer* (SSL) VPN *tunnel*.
		2.i. Bank memastikan penerapan *secure coding* dalam pengembangan sistem dan aplikasi untuk meminimalisasi kerentanan atas sistem dan aplikasi.	Dalam memastikan penerapan *secure coding* dimaksud, Bank paling sedikit: 1) memastikan pengembangan sistem dan aplikasi mengikuti praktik *secure coding* sebagai bagian dari *system development life cycle*; 2) melakukan peninjauan *source code* untuk mendeteksi kerentanan terhadap perangkat lunak, terutama sebelum masuk ke tahap *production*; 3) memastikan kesesuaian praktik *secure coding* dengan standar bahasa pemrograman yang ditetapkan Bank dan lingkungan pengembangan terintegrasi (*integrated development environment)* yang digunakan Bank; dan 4) melakukan reviu dan pengujian secara berkala terhadap keamanan perangkat lunak yang dikembangkan oleh intern Bank maupun pihak ketiga.

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		2.j. Bank memastikan pelaksanaan *patching* berjalan dengan baik serta memastikan keandalan dan kemutakhiran seluruh komponen perangkat lunak, jaringan komunikasi, *database*, dan sistem operasi (*operating system*) Bank.	Dalam memastikan pelaksanaan *patching* berjalan dengan baik, Bank paling sedikit: 1) melakukan penentuan strategi *patching*; 2) melakukan pengujian kesesuaian *patch* sebelum diimplementasikan; 3) memastikan proses *patching* dilakukan dengan tepat waktu (*timely manner*) sesuai dengan tingkat kritikalitas berdasarkan prioritas kebutuhan *patch*; 4) melakukan kaji ulang atas pelaksanaan *patching* untuk memastikan *patching* telah memadai; dan 5) mendokumentasikan proses dan prosedur pengelolaan *patch*.
3.	Proses Deteksi Insiden Siber	3.a. Bank memastikan ketersediaan dokumentasi kinerja dasar (*baseline performance*) atas fungsi kritis Bank dan sistem pendukung, agar setiap penyimpangan dapat dideteksi secara tepat waktu serta aktivitas dan kejadian anomali dapat ditandai untuk ditindaklanjuti.	Dalam memastikan ketersediaan dokumentasi kinerja dasar, Bank paling sedikit: 1) memastikan ketersediaan SDM, proses, dan teknologi yang mampu mendeteksi penyimpangan dari kinerja dasar sistem; 2) memiliki kriteria batasan yang dapat memicu peringatan/tanda ketika terdapat aktivitas atau kejadian anomali; 3) melakukan analisis untuk memahami penyebab kejadian, target dan metode serangan atau kejadian, serta dampak yang dapat ditimbulkan atas suatu kejadian; 4) memastikan bahwa kemampuan deteksi, kinerja dasar sistem, kriteria batasan pemicu, dan peringatan selalu ditinjau dan diperbaharui secara berkala untuk memastikan akurasi dalam pemeriksaan risiko terkait

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			keamanan siber serta tetap sepadan dengan ancaman dan kerentanan siber Bank; 5) melakukan sentralisasi dan mengoordinasikan proses keamanan siber dan teknologi (contoh: *Security Operations Center* (SOC) atau yang sejenis); dan 6) memastikan dokumentasi kinerja dasar disimpan dalam media yang aman dan terdapat *back-up*.
		3.b. Bank melakukan pemantauan atas aktivitas mencurigakan serta melakukan pengelolaan dan pengujian terhadap proses dan prosedur deteksi untuk memastikan aktivitas anomali dapat dideteksi secara tepat waktu.	Dalam melakukan pemantauan atas aktivitas mencurigakan serta melakukan pengelolaan dan pengujian proses maupun prosedur deteksi, Bank paling sedikit: 1) mengimplementasikan *detailed logging* yang mencakup informasi terperinci, seperti *event source*, tanggal, *user*, *timestamp*, *source addresses*, *destination addresses*, dan komponen lain sebagai sumber pemantauan berkelanjutan; 2) mengimplementasikan *Security Information and Event Management* (SIEM) atau *log analytic tools* untuk keperluan dokumentasi, korelasi, dan analisis *log*; 3) melakukan *back-up* terhadap audit *log*, *system log*, dan *configuration log* pada *log server* yang tersentralisasi untuk mencegah akses atau perubahan *log* yang tidak diotorisasi dan memastikan kapasitas penyimpanan *log* sesuai dengan kebutuhan; 4) melakukan deteksi atas akses yang tidak diotorisasi, anomali pada jaringan, serta kegagalan *login* pada perangkat jaringan, server, dan aplikasi; 5) memiliki sistem peringatan atas aktivitas mencurigakan serta ditindaklanjuti dan dikomunikasikan kepada pemangku kepentingan yang relevan; dan

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6) menentukan prioritas atas kejadian (*event*) dalam *log* berdasarkan tingkat keparahan/dampak dan kategori keamanan.
		3.c. Bank melakukan pemantauan atau deteksi secara berkelanjutan terhadap kerentanan untuk memastikan efektivitas upaya pelindungan yang telah diterapkan.	Dalam melakukan pemantauan atau deteksi secara berkelanjutan terhadap kerentanan, Bank paling sedikit: 1) melakukan deteksi terhadap *malicious code*, *unauthorized encryption and mobile code*, dan deteksi *wireless access point* kepada LAN (*ethernet*), serta memahami potensi dampak yang disebabkan oleh peristiwa tersebut; 2) memantau sistem informasi dan aset TI untuk mengidentifikasi peristiwa keamanan siber dan memverifikasi efektivitas tindakan pelindungan yang dilakukan; 3) melakukan upaya untuk mendeteksi adanya *malicious domain* (contoh: penggunaan DNS *query logging* untuk mengetahui adanya *unauthorized domain*); 4) melakukan reviu secara berkala terhadap hasil pengujian berdasarkan analisis kerentanan serta memastikan tindak lanjut atas hasil pengujian; 5) melakukan analisis atas *security control gaps* berdasarkan hasil pengujian; 6) melakukan upaya untuk memperoleh informasi terkini mengenai keamanan siber (contoh: melalui perolehan informasi dari *managed security service provider* atau penyedia produk keamanan siber, *multiple threat intelligence feeds*, dan *cyber threat intelligence unit*); dan 7) menerapkan *early warning system* terhadap anomali pada sistem.

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		3.d. Bank memastikan ketersediaan proses untuk mendeteksi insiden siber secara memadai.	Dalam memastikan ketersediaan proses untuk mendeteksi insiden siber, Bank paling sedikit: 1) memastikan mekanisme deteksi (antivirus dan *anti-malware alerts*, *log event alerts*, perangkat pengamanan) berjalan dengan baik untuk memberikan peringatan atas insiden atau serangan siber; 2) memastikan ketersediaan *log* dari infrastruktur TI yang dapat digunakan untuk analisis; 3) memiliki proses kolaborasi informasi kejadian siber dari berbagai sumber, seperti perangkat lunak, jaringan komunikasi, *database*, dan sistem operasi (*operating system*); 4) memastikan bahwa kemampuan deteksi dan pemantauan dapat menyediakan informasi yang memadai untuk mendukung analisis atas insiden yang terjadi; dan 5) memastikan adanya proses pencatatan terhadap insiden siber yang terdeteksi sesuai dengan kategorisasi insiden siber berdasarkan tingkat keparahan/prioritas/dampak, kategori keamanan, dan jenis *log* yang berkorelasi (contoh: dengan menggunakan *ticketing system*).
		3.e. Bank melakukan analisis terhadap ancaman dan kerentanan dari suatu insiden siber untuk memastikan penanganan insiden secara efektif sehingga dapat mencegah terjadinya gangguan pada	Dalam melakukan analisis terhadap ancaman dan kerentanan dari suatu insiden siber, Bank paling sedikit: 1) menggunakan informasi yang tersedia untuk meningkatkan sistem pengendalian intern dan manajemen risiko terkait keamanan siber Bank; 2) memiliki *escalation profile* untuk setiap insiden siber yang ditemukan dan dilakukan kaji ulang secara

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		layanan dan/atau operasional Bank.	berkala, antara lain mencakup *contact tree* dan *event notification* berdasarkan prioritas; 3) memperoleh atau menyusun informasi mengenai insiden siber yang antara lain terdiri atas *Indicator of Compromise* (IOC) serta informasi yang juga mencakup taktik dan teknik serangan, prosedur atau pola serangan, tindakan mitigasi yang direkomendasikan, serta motivasi/tujuan dan identitas *threat actor*; dan 4) menggunakan *security metrics* untuk mengevaluasi efisiensi penerapan keamanan siber dan melakukan kaji ulang secara berkala.
4.	Proses Penanggulangan dan Pemulihan Insiden Siber	4.a. Bank menetapkan rencana penanggulangan dan pemulihan insiden siber untuk memastikan penanggulangan dan pengembalian layanan yang tepat waktu sesuai dengan risiko yang ditimbulkan, dengan dampak minimal.	Rencana penanggulangan dan pemulihan insiden siber paling sedikit memuat: 1) kategorisasi fungsi kritis sebagaimana proses identifikasi untuk menentukan prioritas pemulihan sistem dan layanan; 2) rencana *re-route* atau penggantian fungsi kritis yang terdampak insiden siber; 3) pelaporan dan eskalasi di intern Bank, termasuk kepada pejabat eksekutif, Direksi, dan Dewan Komisaris, berdasarkan potensi dampak dari insiden siber; 4) peran dan tanggung jawab yang jelas untuk seluruh pegawai yang terlibat dalam proses eskalasi, penanggulangan, dan pemulihan insiden siber; dan 5) jalur komunikasi kepada pemangku kepentingan intern dan ekstern yang perlu dikomunikasikan tentang insiden siber dan praktik/teknik serangan siber yang berkembang saat ini yang berpotensi meningkatkan

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			risiko terjadinya *fraud*, termasuk waktu pemberitahuan, dan cakupan informasi yang perlu dikomunikasikan. Tingkat keterlibatan pemangku kepentingan ditentukan oleh tingkat keparahan dan dampak insiden siber. Dalam menyusun rencana penanggulangan dan pemulihan dimaksud, Bank: 1) mempertimbangkan berbagai skenario insiden siber dalam merumuskan rencana penanggulangan dan pemulihan serta melakukan analisis dampak atas insiden siber terhadap aktivitas Bank; dan 2) memastikan rencana penanggulangan dan pemulihan sesuai dengan rencana kelangsungan usaha (*business continuity plan*), rencana pemulihan bencana (*disaster recovery plan*), *crisis management plan*, dan/atau kebijakan atau rencana Bank lainnya yang terkait.
		4.b. Bank menetapkan peran serta tugas dan tanggung jawab tim tanggap insiden siber untuk memastikan penanggulangan dan pemulihan insiden siber dilaksanakan dengan dampak minimal terhadap layanan dan operasional Bank.	
		4.c. Bank menerapkan prosedur pemulihan dan upaya untuk mencegah penyebaran dampak dari suatu insiden siber dengan memitigasi dampak dan	Dalam menerapkan prosedur pemulihan dan upaya untuk mencegah penyebaran dampak dari suatu insiden, Bank paling sedikit: 1) memastikan pemahaman terhadap dampak dari insiden siber, pelaksanaan pemeriksaan forensik, dan kategorisasi insiden siber;

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		menanggulangi insiden siber tersebut.	2) melakukan langkah penanggulangan dan pemulihan insiden siber sesuai dengan rencana; 3) melakukan *root cause analysis* terhadap insiden siber untuk mencegah terulangnya kejadian serupa; dan 4) melakukan kaji ulang terhadap rekapitulasi laporan insiden siber untuk mempelajari kesesuaian prosedur insiden siber dengan standar dan prosedur yang telah ditetapkan.
		4.d. Bank melakukan analisis untuk memastikan langkah penanggulangan dan pemulihan insiden siber dijalankan dengan tepat.	Dalam melakukan analisis, Bank paling sedikit: 1) menerapkan isolasi insiden siber sebagai langkah mitigasi awal; 2) mengimplementasikan rencana *re-route* atau penggantian fungsi kritis yang terdampak insiden siber; 3) melakukan upaya untuk mengembalikan operasional dengan gangguan layanan yang minimal sesuai dengan jenis insiden siber yang terjadi; dan 4) memiliki prosedur untuk memastikan aset TI yang terdampak oleh insiden siber dan tidak dapat digunakan kembali untuk kegiatan operasional telah digantikan, sehingga fungsi operasional tetap berjalan.
		4.e. Bank melakukan eskalasi dan pelaporan atas insiden siber sesuai dengan jalur komunikasi yang telah ditetapkan.	Dalam melakukan eskalasi dan pelaporan atas insiden siber sesuai dengan jalur komunikasi yang telah ditetapkan, Bank paling sedikit: 1) memiliki *ticketing system* yang digunakan untuk melacak perkembangan terkini dari penanggulangan dan pemulihan yang dilakukan (*event post-notification*) serta mengategorisasikan kejadian berdasarkan tingkat keparahan/prioritas/dampak, kategori keamanan, dan jenis *log* yang berkorelasi;

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			2) menetapkan prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber; 3) melakukan eskalasi untuk melaporkan pelaksanaan penanggulangan dan pemulihan insiden siber kepada pejabat eksekutif, Direksi, dan Dewan Komisaris berdasarkan kriteria potensi dampak dan kritikalitas; 4) melakukan eskalasi kepada pihak yang berwenang untuk melakukan penanggulangan dan analisis insiden siber sesuai dengan *service level agreement* tertentu; dan 5) memiliki prosedur dan melakukan komunikasi kepada nasabah dan pihak lain yang terkait (termasuk media dalam hal diperlukan) ketika terjadi insiden siber yang dapat menyebabkan gangguan atau penurunan layanan Bank kepada nasabah.
		4.f. Bank melakukan analisis pascainsiden sebagai bahan pelajaran terpetik (*lesson learned*) dalam penanggulangan dan pemulihan insiden siber untuk perbaikan berkelanjutan.	Dalam melakukan analisis pascainsiden, Bank paling sedikit: 1) menyusun prosedur untuk mendapatkan pelajaran terpetik (*lesson learned*) sebagai bahan perbaikan di masa depan; dan 2) mencatat setiap langkah yang dilakukan dalam penanggulangan insiden siber sebagai pelajaran terpetik (*lesson learned*) dari insiden siber yang terjadi untuk meningkatkan kapabilitas mitigasi risiko serta penginian terhadap rencana penanggulangan dan pemulihan insiden siber Bank apabila diperlukan.

Ditetapkan di Jakarta

pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN

OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN II

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

II.a. Kertas Kerja Penilaian Risiko Inheren terkait Keamanan Siber

Penilaian Risiko Inheren terkait Keamanan Siber untuk Faktor Teknologi

1. Teknologi		**Level Risiko**					**Hasil Penilaian[1)]**	**Penjelasan[2)]**
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
1.1.	Interkoneksi ke internet publik	Kurang atau sama dengan 2 koneksi	4 koneksi	6 koneksi	8 koneksi	Lebih atau sama dengan 10 koneksi		
1.2.	Interkoneksi ke pihak ketiga (*third party*)	Lebih dari 80% total koneksi ke pihak ketiga menggunakan *Application Programming Interface* (API)	Hingga 50% dari total koneksi ke pihak ketiga menggunakan API	Lebih dari 80% total koneksi ke pihak ketiga menggunakan *host to host*	Hingga 50% total koneksi ke pihak ketiga menggunakan *host to host*	Lebih dari 50% total koneksi ke pihak ketiga menggunakan *direct connection*		
1.3.	Akses ke aset TI Bank	Koneksi kabel hanya untuk pegawai	Koneksi kabel untuk pegawai saja dan *Wi-Fi* untuk pihak ketiga terotorisasi	Seluruh koneksi untuk pegawai dan pihak ketiga terotorisasi	Seluruh koneksi untuk pegawai dan pihak ketiga terotorisasi, namun *Wi-Fi* untuk publik	Seluruh koneksi untuk semua pihak		
1.4.	Jaringan intranet dari jaringan kantor Bank	Bank memiliki jaringan kantor Bank yang	Bank memiliki jaringan kantor Bank yang tersebar di 100	Bank memiliki jaringan kantor Bank yang tersebar di	Bank memiliki jaringan kantor Bank yang tersebar di	Bank memiliki jaringan kantor Bank yang tersebar		

1. Teknologi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
		tersebar kurang dari 100 lokasi	hingga 300 lokasi	lebih dari 300 hingga 500 lokasi	lebih dari 500 hingga 700 lokasi	di lebih dari 700 lokasi		
1.5.	Penggunaan pihak penyedia jasa TI dalam penyelenggaraan pusat data	Tidak ada penggunaan jasa pihak penyedia jasa TI dalam penyelenggaraan pusat data	Penggunaan jasa pihak penyedia jasa TI selain *cloud service provider* dalam penyelenggaraan pusat data	Penggunaan jasa *cloud service provider* berupa SaaS	Penggunaan jasa *cloud service provider* berupa PaaS	Penggunaan jasa *cloud service provider* berupa IaaS		
1.6.	Pengelolaan perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* dan TI)	Seluruh perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI) dikelola (dikembangkan	Lebih dari 70% perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI) dikelola (dikembangkan	Lebih dari 50% perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI)	Lebih dari 30% perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI)	Hingga 30% perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office*		

1. Teknologi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
		dan diselenggarakan) oleh tim TI Bank	dan diselenggarakan) oleh tim TI Bank	dikelola (dikembangkan dan diselenggara-kan) oleh tim TI Bank	dikelola (dikembangkan dan diselenggara-kan) oleh tim TI Bank	dan TI) dikelola (dikembang-kan dan diselenggara-kan) oleh tim TI Bank		
1.7.	Penggunaan perangkat keras dan/atau perangkat lunak yang sudah masuk/mendekati masa EOL	Tidak ada perangkat keras dan/atau perangkat lunak yang melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Hingga 30% perangkat keras dan/atau perangkat lunak melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Hingga 50% perangkat keras dan/atau perangkat lunak melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Hingga 70% perangkat keras dan/atau perangkat lunak melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Lebih dari 70% perangkat keras dan/atau perangkat lunak melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)		

1. Teknologi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
1.8.	Jumlah pegawai yang memiliki akses koneksi perangkat pribadi ke jaringan Bank (*Bring Your Own Device*)	Tidak terdapat akses koneksi perangkat pribadi ke jaringan Bank	Akses koneksi perangkat pribadi ke jaringan Bank dimiliki oleh kurang dari 5% pegawai	Akses koneksi perangkat pribadi ke jaringan Bank dimiliki oleh kurang dari 10% pegawai	Akses koneksi perangkat pribadi ke jaringan Bank dimiliki oleh kurang dari 25% pegawai	Akses koneksi perangkat pribadi ke jaringan Bank dimiliki oleh 25% pegawai atau lebih		
1.9.	Perangkat lunak yang dapat diakses menggunakan perangkat pribadi ke jaringan Bank	Tidak terdapat perangkat lunak yang dapat diakses menggunakan perangkat pribadi	Perangkat pribadi yang terhubung ke jaringan Bank hanya dapat mengakses surat elektronik	Perangkat pribadi yang terhubung ke jaringan Bank hanya dapat mengakses surat elektronik dan aplikasi penunjang (tidak bersifat kritikal)	Perangkat pribadi yang terhubung ke jaringan Bank dapat mengakses aplikasi kritikal	Perangkat pribadi yang terhubung ke jaringan Bank dapat mengakses seluruh sistem/aplikasi (termasuk *core banking system*)		
1.10.	Pihak ketiga yang memiliki akses terhadap sistem internal Bank dan/atau informasi sensitif	Tidak terdapat pihak ketiga atau individu dari pihak ketiga yang memiliki akses terhadap	Jumlah minimal (1 – 3 entitas atau kurang dari 10 individu) memiliki akses terhadap sistem	Jumlah sedang (4 – 6 entitas atau kurang dari 20 individu) memiliki akses	Jumlah signifikan (7 – 10 entitas atau kurang dari 30 individu) memiliki akses	Jumlah substansial (Lebih dari 10 entitas atau 30 individu atau lebih)		

1. Teknologi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
		sistem internal Bank dan/atau informasi sensitif	internal Bank dan/atau informasi sensitif	terhadap sistem internal Bank dan/atau informasi sensitif	terhadap sistem internal Bank dan/atau informasi sensitif	memiliki akses terhadap sistem internal Bank dan/atau informasi sensitif		

Keterangan:

1) Diisi dengan angka 1 (satu) sampai 5 (lima) sesuai dengan kondisi Bank pada saat penilaian dilakukan.

2) Diisi dengan penjelasan dari hasil penilaian yang dilakukan oleh Bank.

Penilaian Risiko Inheren terkait Keamanan Siber untuk Faktor Produk Bank

2. **Produk Bank**		**Level Risiko**					**Hasil Penilaian[1)]**	**Penjelasan[2)]**
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
2.1.	Penggunaan saluran daring dan *mobile* dalam memberikan layanan	Tidak ada aplikasi (baik *back-office* maupun untuk nasabah) yang menggunakan saluran daring dan *mobile*	Saluran daring dan *mobile* digunakan untuk penyampaian informasi umum Bank kepada masyarakat (antara lain notifikasi/berita, lokasi jaringan kantor, dan produk Bank yang tersedia)	Saluran daring dan *mobile* digunakan untuk pelayanan transaksi perbankan (produk Bank) bagi nasabah badan usaha secara domestik	Saluran daring dan *mobile* digunakan untuk pelayanan transaksi perbankan (produk Bank) bagi nasabah ritel secara domestik	Saluran daring dan *mobile* digunakan untuk: 1. kebutuhan produk bagi nasabah badan usaha dan ritel termasuk remitansi luar negeri dan pertukaran mata uang; dan/atau 2. interkoneksi dengan ekosistem ekonomi digital (contoh: *super app*)		
2.2.	Mekanisme pengelolaan ATM	Bank tidak memiliki layanan ATM	Layanan ATM tersedia, namun Bank tidak	Layanan ATM tersedia, mesin ATM dan proses	Layanan ATM tersedia, mesin ATM dan proses	Layanan ATM tersedia, mesin ATM dan pengisian uang		

2. Produk Bank		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		Low (1)	*Low to Moderate* (2)	*Moderate* (3)	*Moderate to High* (4)	*High* (5)		
			memiliki mesin ATM sendiri	pengisian uang dikelola sepenuhnya oleh Bank	pengisian uang dikelola dengan kombinasi antara Bank dan pihak ketiga	dikelola sepenuhnya oleh pihak ketiga		
2.3.	Produk Bank berupa APMK	Bank tidak menerbitkan APMK	Bank hanya menerbitkan APMK berupa kartu debit untuk mendukung layanan Bank tersebut	Bank menerbitkan APMK (kartu debit dan APMK lainnya) hanya untuk mendukung layanan Bank tersebut	Bank menerbitkan APMK untuk 1 hingga 5 bank lain/institusi keuangan lain	Bank menerbitkan APMK untuk lebih dari 5 bank lain/institusi keuangan lain		
2.4.	Jenis produk Bank berbasis TI	Bank tidak memiliki produk Bank berbasis TI	Bank memiliki produk Bank berbasis TI untuk penghimpunan dan/atau penyaluran dana	Bank memiliki produk Bank berbasis TI untuk penghimpunan dana, penyaluran dana,	Bank memiliki produk Bank berbasis TI untuk penghimpunan dana, penyaluran dana, *treasury*,	Bank memiliki produk Bank berbasis TI untuk penghimpunan dana, penyaluran dana, *treasury*, dan/atau aktivitas sistem		

2. Produk Bank		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		Low (1)	*Low to Moderate* (2)	*Moderate* (3)	*Moderate to High* (4)	*High* (5)		
				dan/atau *treasury*	dan/atau aktivitas sistem pembayaran dan investasi pasar modal untuk kebutuhan domestik	pembayaran termasuk jual beli mata uang dan investasi pasar modal untuk kebutuhan internasional		
2.5.	Bank sebagai penyedia jasa TI	Bank tidak menjadi penyedia jasa TI untuk lembaga jasa keuangan lain	Bank menjadi penyedia jasa TI untuk 1 atau 2 lembaga jasa keuangan lain	Bank menjadi penyedia jasa TI untuk 3 lembaga jasa keuangan lain	Bank menjadi penyedia jasa TI untuk 4 atau 5 lembaga jasa keuangan lain	Bank menjadi penyedia jasa TI untuk lebih dari 5 lembaga jasa keuangan lain		

Keterangan:

1) Diisi dengan angka 1 (satu) sampai 5 (lima) sesuai dengan kondisi Bank pada saat penilaian dilakukan.

2) Diisi dengan penjelasan dari hasil penilaian yang dilakukan oleh Bank.

Penilaian Risiko Inheren terkait Keamanan Siber untuk Faktor Karakteristik Organisasi

3. Karakteristik Organisasi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
3.1.	Pergantian (*turnover*) pada SDM yang menangani TI/ ketahanan dan keamanan siber	Persentase pergantian SDM yang menangani TI/ ketahanan dan keamanan siber <5% dalam 1 tahun terakhir	Persentase pergantian SDM yang menangani TI/ ketahanan dan keamanan siber <10% dalam 1 tahun terakhir	Persentase pergantian SDM yang menangani TI/ ketahanan dan keamanan siber <15% dalam 1 tahun terakhir	Persentase pergantian SDM yang menangani TI/ ketahanan dan keamanan siber < 20% dalam 1 tahun terakhir	Persentase pergantian SDM yang menangani TI/ ketahanan dan keamanan siber ≥ 20% dalam 1 tahun terakhir		
3.2.	Perubahan di lingkungan TI	Kurang dari 3 implementasi sistem kritikal dalam 1 tahun terakhir	3-5 implementasi sistem kritikal dalam 1 tahun terakhir	6-8 implementasi sistem kritikal dalam 1 tahun terakhir	9-11 implementasi sistem kritikal dalam 1 tahun terakhir	>11 implementasi sistem kritikal dalam 1 tahun terakhir		
3.3.	Pengelolaan *privilege access* (administrator dan selevel administrator) di	Seluruh *privilege access* untuk seluruh tipe perangkat	*Privilege access* untuk 1 atau 2 tipe perangkat	*Privilege access* untuk 3 tipe perangkat	*Privelege access* untuk 4 tipe perangkat	*Privelege access* untuk lebih dari 4 tipe perangkat dikelola oleh		

3. Karakteristik Organisasi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
	seluruh perangkat (*host*, jaringan, *database*, aplikasi, dan *cloud*)	dikelola oleh unit TI	dikelola oleh pihak selain unit TI	dikelola oleh pihak selain unit TI	dikelola oleh pihak selain unit TI	pihak selain unit TI		

Keterangan:

1) Diisi dengan angka 1 (satu) sampai 5 (lima) sesuai dengan kondisi Bank pada saat penilaian dilakukan.
2) Diisi dengan penjelasan dari hasil penilaian yang dilakukan oleh Bank.

Penilaian Risiko Inheren terkait Keamanan Siber untuk Faktor Karakteristik Rekam Jejak Insiden Siber

4. Rekam Jejak Insiden Siber		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
4.1	Persentase insiden siber yang berdampak signifikan dalam 12 (dua belas) bulan terakhir	Tidak ada insiden siber yang berdampak signifikan	Hingga 30% dari total insiden siber berdampak signifikan	Hingga 50% dari total insiden siber berdampak signifikan	Hingga 70% dari total insiden siber berdampak signifikan	Lebih dari 70% dari total insiden siber berdampak signifikan		
4.2	Cakupan dampak insiden siber dalam 12 (dua belas) bulan terakhir	Tidak terdapat dampak (tidak terdapat insiden siber)	Insiden siber hanya berdampak pada internal Bank	Insiden siber berdampak pada pihak ketiga selain nasabah	Insiden siber berdampak pada ketersediaan produk Bank	Insiden siber berdampak pada kerugian nasabah (contoh: kebocoran data pribadi nasabah)		

Keterangan:

1) Diisi dengan angka 1 (satu) sampai 5 (lima) sesuai dengan kondisi Bank pada saat penilaian dilakukan.

2) Diisi dengan penjelasan dari hasil penilaian yang dilakukan oleh Bank.

II.b. Kertas Kerja Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber

No.	Domain[1)]	Subdomain[1)]	Kontrol[1)]	Penerapan Kontrol[2)]	Penjelasan[3)]	Referensi Dokumen[4)]	Departemen/Unit/Jabatan yang Bertanggung Jawab
1.	Tata Kelola Risiko terkait Keamanan Siber	1.1. Kecukupan Pengawasan Aktif oleh Direksi dan Dewan Komisaris	1.1.a. Bank menetapkan wewenang dan tanggung jawab Direksi terkait dengan penerapan manajemen risiko terkait keamanan siber.				
…	…	…	…				
…	…	…	…				

Keterangan:

1) Diisi dengan domain, subdomain, dan kontrol sebagaimana tercantum dalam Lampiran I.b. Matriks Kontrol Penerapan Manajemen Risiko terkait Keamanan Siber.
2) Diisi dengan penilaian atas kondisi penerapan kontrol pada Bank, yaitu: "**Belum Diterapkan**", "**Belum Memadai**", "**Cukup Memadai**", "**Memadai**", atau "**Sangat Memadai**". Penilaian mempertimbangkan penjelasan/kriteria pemenuhan kontrol sebagaimana tercantum dalam Lampiran I.b. Matriks Kontrol Penerapan Manajemen Risiko terkait Keamanan Siber.
3) Diisi dengan penjelasan atas kondisi penerapan kontrol (jika ada).
4) Diisi dengan dokumen yang dapat dijadikan acuan dalam menilai penerapan kontrol.

II.c. Kertas Kerja Penilaian Kualitas Penerapan Proses Ketahanan Siber

No.	Domain[1)]	Kontrol[1)]	Penerapan Kontrol[2)]	Penjelasan[3)]	Referensi Dokumen[4)]	Departemen/Unit/ Jabatan yang Bertanggung Jawab
1.	Proses Identifikasi Aset, Ancaman, dan Kerentanan	1.a. Bank menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta pencatatan konfigurasi secara efektif.				
...	...	...				
...	...	...				

Keterangan:

1) Diisi dengan domain dan kontrol sebagaimana tercantum dalam Lampiran I.c. Matriks Kontrol Penerapan Proses Ketahanan Siber.
2) Diisi dengan penilaian atas kondisi penerapan kontrol pada Bank, yaitu: "**Belum Diterapkan**", "**Belum Memadai**", "**Cukup Memadai**", "**Memadai**", atau "**Sangat Memadai**". Penilaian mempertimbangkan penjelasan/kriteria pemenuhan kontrol sebagaimana tercantum dalam Lampiran I.c. Matriks Kontrol Penerapan Proses Ketahanan Siber.
3) Diisi dengan penjelasan atas kondisi penerapan kontrol (jika ada).
4) Diisi dengan dokumen yang dapat dijadikan acuan dalam menilai penerapan kontrol.

Ditetapkan di Jakarta
pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN III

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

III.a. Matriks Penetapan Tingkat Risiko Inheren terkait Keamanan Siber

Peringkat	Definisi Peringkat
Low (1)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Bank, kemungkinan kerugian yang dihadapi Bank dari risiko inheren terkait keamanan siber tergolong sangat rendah selama periode waktu tertentu pada masa depan. Contoh karakteristik Bank yang termasuk dalam peringkat *Low* (1): a. Bank menggunakan TI yang sangat terbatas dan kerentanan terhadap serangan siber sangat rendah; b. tidak terdapat produk Bank yang disalurkan menggunakan TI dan/atau saluran daring dan *mobile*; c. pergantian (*turnover*) pada SDM yang menangani TI/ ketahanan dan keamanan siber sangat rendah; d. tidak terdapat insiden siber yang berdampak signifikan selama 12 (dua belas) bulan terakhir.
Low to Moderate (2)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Bank, kemungkinan kerugian yang dihadapi Bank dari risiko inheren terkait keamanan siber tergolong rendah selama periode waktu tertentu pada masa depan. Contoh karakteristik Bank yang termasuk dalam peringkat *Low to Moderate* (2): a. Bank menggunakan TI yang terbatas, kerentanan terhadap serangan siber rendah, dan Bank melakukan *outsourcing* TI dengan kompleksitas yang sangat rendah; b. jenis produk Bank yang disalurkan menggunakan TI dan/atau saluran daring dan *mobile* sangat terbatas; c. pergantian (*turnover*) pada SDM yang menangani TI/ketahanan dan keamanan siber rendah; d. persentase insiden siber yang berdampak signifikan selama 12 (dua belas) bulan terakhir sangat rendah serta berdampak hanya pada intern Bank.
Moderate (3)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Bank, kemungkinan kerugian yang dihadapi Bank dari risiko inheren terkait keamanan siber tergolong cukup tinggi selama periode waktu tertentu pada masa depan. Contoh karakteristik Bank yang termasuk dalam peringkat *Moderate* (3): a. Bank menggunakan TI yang cukup terbatas, kerentanan terhadap serangan siber cukup rendah, dan Bank melakukan *outsourcing* TI dengan kompleksitas yang rendah; b. jenis produk Bank yang disalurkan menggunakan TI dan/atau saluran daring dan *mobile* terbatas; c. pergantian (*turnover*) pada SDM yang menangani TI/ ketahanan dan keamanan siber cukup tinggi; d. persentase insiden siber yang berdampak signifikan selama 12 (dua belas) bulan terakhir rendah serta berdampak pada pihak ketiga selain nasabah.

Peringkat	Definisi Peringkat
Moderate to High (4)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Bank, kemungkinan kerugian yang dihadapi Bank dari risiko inheren terkait keamanan siber tergolong tinggi selama periode waktu tertentu pada masa depan. Contoh karakteristik Bank yang termasuk dalam peringkat *Moderate to High* (4): a. Bank menggunakan TI yang kompleks dalam hal cakupan dan kecanggihannya, kerentanan terhadap serangan siber cukup tinggi, dan Bank melakukan *outsourcing* TI kritikal dengan kompleksitas yang cukup tinggi; b. jenis produk Bank yang disalurkan menggunakan TI dan/atau saluran daring dan *mobile* cukup banyak; c. pergantian (*turnover*) pada SDM yang menangani TI/ ketahanan dan keamanan siber tinggi; d. persentase insiden siber yang berdampak signifikan selama 12 (dua belas) bulan terakhir cukup tinggi serta berdampak pada ketersediaan produk Bank.
High (5)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Bank, kemungkinan kerugian yang dihadapi Bank dari risiko inheren terkait keamanan siber tergolong sangat tinggi selama periode waktu tertentu pada masa depan. Contoh karakteristik Bank yang termasuk dalam peringkat *High* (5): a. Bank menggunakan TI yang sangat kompleks dalam hal cakupan dan kecanggihannya, kerentanan terhadap serangan siber sangat tinggi, dan Bank melakukan *outsourcing* TI kritikal dengan kompleksitas yang tinggi; b. jenis produk Bank yang disalurkan menggunakan TI dan/atau saluran daring dan *mobile* sangat tinggi; c. pergantian (*turnover*) pada SDM yang menangani TI/ ketahanan dan keamanan siber sangat tinggi; d. persentase insiden siber yang berdampak signifikan selama 12 (dua belas) bulan terakhir sangat tinggi serta berdampak langsung pada kerugian nasabah.

III.b. Matriks Penetapan Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber

Peringkat	Definisi Peringkat
Strong (1)	Kualitas penerapan manajemen risiko terkait keamanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat *Strong* (1): a. pengawasan aktif oleh Direksi dan Dewan Komisaris secara keseluruhan sangat memadai; b. SDM sangat memadai, baik dari sisi kuantitas maupun kompetensi pada fungsi manajemen risiko terkait keamanan siber; c. struktur organisasi terkait penerapan manajemen risiko terkait keamanan siber pada seluruh satuan kerja telah berjalan dengan sangat baik; d. Direksi dan Dewan Komisaris memiliki kesadaran (*awareness*) dan pemahaman mengenai manajemen risiko terkait keamanan siber yang sangat baik; e. budaya dan kesadaran manajemen risiko terkait keamanan siber telah dikembangkan dan diimplementasikan dengan sangat baik di seluruh lingkungan organisasi Bank; f. program peningkatan kapasitas SDM di bidang keamanan informasi dan manajemen risiko terkait keamanan siber sangat memadai; g. penetapan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) sangat memadai serta sangat sesuai dengan sasaran strategis dan strategi bisnis Bank; h. strategi manajemen risiko terkait keamanan siber sangat sejalan dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber; i. kebijakan dan prosedur manajemen risiko serta penetapan limit risiko terkait keamanan siber sangat memadai dan tersedia untuk seluruh area manajemen risiko terkait keamanan siber, sejalan dengan penerapan, dan dipahami dengan baik oleh pegawai; j. proses manajemen risiko terkait keamanan siber sangat memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan risiko terkait keamanan siber; k. sistem informasi manajemen risiko terkait keamanan siber sangat baik sehingga menghasilkan laporan risiko terkait keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris; l. sistem pengendalian intern sangat efektif dalam mendukung pelaksanaan manajemen risiko terkait keamanan siber; m. pelaksanaan kaji ulang independen oleh satuan kerja audit intern dan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber sangat memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris;

Peringkat	Definisi Peringkat
	n. secara umum tidak terdapat kelemahan yang signifikan berdasarkan hasil kaji ulang independen; o. tindak lanjut atas kaji ulang independen telah dilaksanakan dengan sangat memadai.
Satisfactory (2)	Kualitas penerapan manajemen risiko terkait keamanan siber memadai. Meskipun terdapat beberapa kelemahan minor, kelemahan tersebut dapat diselesaikan pada aktivitas bisnis normal. Contoh karakteristik Bank yang termasuk dalam peringkat *Satisfactory* (2): a. pengawasan aktif oleh Direksi dan Dewan Komisaris secara keseluruhan memadai; b. SDM memadai, baik dari sisi kuantitas maupun kompetensi pada fungsi manajemen risiko terkait keamanan siber; c. struktur organisasi terkait penerapan manajemen risiko terkait keamanan siber pada seluruh satuan kerja telah berjalan dengan baik; d. Direksi dan Dewan Komisaris memiliki kesadaran (*awareness*) dan pemahaman mengenai manajemen risiko terkait keamanan siber yang baik; e. budaya dan kesadaran manajemen risiko terkait keamanan siber telah dikembangkan dan diimplementasikan dengan baik di seluruh lingkungan organisasi Bank; f. program peningkatan kapasitas SDM di bidang keamanan informasi dan manajemen risiko terkait keamanan siber memadai; g. penetapan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) memadai serta sesuai dengan sasaran strategis dan strategi bisnis Bank; h. strategi manajemen risiko terkait keamanan siber sejalan dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber; i. kebijakan dan prosedur manajemen risiko serta penetapan limit risiko terkait keamanan siber memadai dan tersedia untuk seluruh area manajemen risiko terkait keamanan siber, sejalan dengan penerapan, dan dipahami dengan baik oleh pegawai meskipun terdapat kelemahan minor; j. proses manajemen risiko terkait keamanan siber memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan risiko terkait keamanan siber; k. sistem informasi manajemen risiko terkait keamanan siber baik sehingga menghasilkan laporan risiko terkait keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris; l. sistem pengendalian intern efektif dalam mendukung pelaksanaan manajemen risiko terkait keamanan siber; m. pelaksanaan kaji ulang independen oleh satuan kerja audit intern dan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris; n. terdapat kelemahan yang tidak signifikan berdasarkan hasil kaji ulang independen;

Peringkat	Definisi Peringkat
	o. tindak lanjut atas kaji ulang independen telah dilaksanakan dengan memadai.
Fair (3)	Kualitas penerapan manajemen risiko terkait keamanan siber cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen. Contoh karakteristik Bank yang termasuk dalam peringkat *Fair* (3): a. pengawasan aktif oleh Direksi dan Dewan Komisaris secara keseluruhan cukup memadai; b. SDM cukup memadai, baik dari sisi kuantitas maupun kompetensi pada fungsi manajemen risiko terkait keamanan siber; c. struktur organisasi terkait penerapan manajemen risiko terkait keamanan siber pada seluruh satuan kerja telah berjalan dengan cukup baik; d. Direksi dan Dewan Komisaris memiliki kesadaran (*awareness*) dan pemahaman mengenai manajemen risiko terkait keamanan siber yang cukup baik; e. budaya dan kesadaran manajemen risiko terkait keamanan siber telah dikembangkan dan diimplementasikan dengan cukup baik di seluruh lingkungan organisasi Bank; f. program peningkatan kapasitas SDM di bidang keamanan informasi dan manajemen risiko terkait keamanan siber cukup memadai; g. penetapan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) cukup memadai namun tidak selalu sesuai dengan sasaran strategis dan strategi bisnis Bank; h. strategi manajemen risiko terkait keamanan siber cukup sejalan dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber; i. kebijakan dan prosedur manajemen risiko serta penetapan limit risiko terkait keamanan siber cukup memadai namun tidak selalu sejalan dengan penerapan; j. proses manajemen risiko terkait keamanan siber cukup memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan risiko terkait keamanan siber; k. sistem informasi manajemen risiko terkait keamanan siber cukup baik, termasuk pelaporan risiko terkait keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris; l. sistem pengendalian intern cukup efektif dalam mendukung pelaksanaan manajemen risiko terkait keamanan siber; m. pelaksanaan kaji ulang independen oleh satuan kerja audit intern dan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber cukup memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris; n. terdapat kelemahan yang cukup signifikan berdasarkan hasil kaji ulang independen yang memerlukan perhatian manajemen;

Peringkat	Definisi Peringkat
	o. tindak lanjut atas kaji ulang independen telah dilaksanakan dengan cukup memadai.
Marginal (4)	Kualitas penerapan manajemen risiko terkait keamanan siber kurang memadai. Terdapat kelemahan signifikan pada berbagai aspek manajemen risiko terkait keamanan siber yang memerlukan tindakan korektif segera. Contoh karakteristik Bank yang termasuk dalam peringkat *Marginal* (4): a. pengawasan aktif oleh Direksi dan Dewan Komisaris secara keseluruhan kurang memadai, dan terdapat kelemahan pada berbagai aspek penilaian yang memerlukan perbaikan segera; b. SDM kurang memadai, baik dari sisi kuantitas maupun kompetensi pada fungsi manajemen risiko terkait keamanan siber; c. struktur organisasi terkait penerapan manajemen risiko terkait keamanan siber pada seluruh satuan kerja kurang berjalan dengan baik; d. kelemahan signifikan atas kesadaran (*awareness*) dan pemahaman Direksi dan Dewan Komisaris mengenai manajemen risiko terkait keamanan siber; e. budaya dan kesadaran manajemen risiko terkait keamanan siber kurang dikembangkan dan diimplementasikan dengan baik di seluruh lingkungan organisasi Bank; f. program peningkatan kapasitas SDM di bidang keamanan informasi dan manajemen risiko terkait keamanan siber kurang memadai; g. penetapan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) kurang memadai serta tidak sesuai dengan sasaran strategis dan strategi bisnis Bank; h. strategi manajemen risiko terkait keamanan siber kurang sejalan dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber; i. kebijakan dan prosedur manajemen risiko serta penetapan limit risiko terkait keamanan siber kurang memadai dan tidak sejalan dengan penerapan; j. proses manajemen risiko terkait keamanan siber kurang memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan risiko terkait keamanan siber; k. kelemahan signifikan pada sistem informasi manajemen risiko terkait keamanan siber, termasuk pelaporan risiko terkait keamanan siber kepada Direksi dan Dewan Komisaris, yang memerlukan perbaikan segera; l. sistem pengendalian intern kurang efektif dalam mendukung pelaksanaan manajemen risiko terkait keamanan siber; m. pelaksanaan kaji ulang independen oleh satuan kerja audit intern dan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber kurang memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris;

Peringkat	Definisi Peringkat
	n. terdapat kelemahan yang signifikan berdasarkan hasil kaji ulang independen yang memerlukan perbaikan segera; o. tindak lanjut atas kaji ulang independen dilaksanakan dengan kurang memadai.
Unsatisfactory (5)	Kualitas penerapan manajemen risiko terkait keamanan siber tidak memadai. Terdapat kelemahan signifikan pada berbagai aspek manajemen risiko terkait keamanan siber yang tindakan penyelesaiannya di luar kemampuan manajemen. Contoh karakteristik Bank yang termasuk dalam peringkat *Unsatisfactory* (5): a. pengawasan aktif oleh Direksi dan Dewan Komisaris secara keseluruhan tidak memadai serta terdapat kelemahan pada hampir seluruh aspek penilaian dan tindakan penyelesaiannya di luar kemampuan Bank; b. SDM tidak memadai, baik dari sisi kuantitas maupun kompetensi pada fungsi manajemen risiko terkait keamanan siber; c. struktur organisasi terkait penerapan manajemen risiko terkait keamanan siber pada seluruh satuan kerja tidak berjalan dengan baik; d. kesadaran (*awareness*) dan pemahaman Direksi dan Dewan Komisaris mengenai manajemen risiko terkait keamanan siber sangat lemah; e. budaya dan kesadaran manajemen risiko terkait keamanan siber tidak dikembangkan dan diimplementasikan di lingkungan organisasi Bank atau belum ada sama sekali; f. program peningkatan kapasitas SDM di bidang keamanan informasi dan manajemen risiko terkait keamanan siber tidak memadai; g. penetapan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) tidak memadai serta tidak terdapat kaitan dengan sasaran strategis dan strategi bisnis Bank; h. strategi manajemen risiko terkait keamanan siber tidak sejalan dengan tingkat risiko yang akan diambil (*risk appetite*) dan toleransi risiko (*risk tolerance*) terkait keamanan siber; i. kelemahan sangat signifikan pada kebijakan dan prosedur manajemen risiko serta penetapan limit risiko terkait keamanan siber; j. proses manajemen risiko terkait keamanan siber tidak memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan risiko terkait keamanan siber; k. kelemahan fundamental pada sistem informasi manajemen risiko terkait keamanan siber; l. sistem pengendalian intern tidak efektif dalam mendukung pelaksanaan manajemen risiko terkait keamanan siber; m. pelaksanaan kaji ulang independen oleh satuan kerja audit intern dan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber tidak memadai, serta terdapat kelemahan pada metodologi, frekuensi, dan/atau pelaporan kepada Direksi dan Dewan Komisaris yang memerlukan perbaikan fundamental;

Peringkat	Definisi Peringkat
	n. terdapat kelemahan yang sangat signifikan berdasarkan hasil kaji ulang independen yang memerlukan perbaikan segera; o. tindak lanjut atas kaji ulang independen tidak memadai atau tidak ada.

III.c. Matriks Penetapan Kualitas Penerapan Proses Ketahanan Siber

Peringkat	Definisi Peringkat
Strong (1)	Kualitas penerapan proses ketahanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat *Strong* (1): a. proses identifikasi aset, ancaman dan kerentanan sangat memadai; b. proses pelindungan aset dilaksanakan dengan sangat baik; c. proses deteksi insiden siber sangat andal dan teruji; d. proses penanggulangan dan pemulihan insiden siber dilaksanakan dengan sangat baik dan tidak menimbulkan gangguan yang signifikan.
Satisfactory (2)	Kualitas penerapan proses ketahanan siber memadai. Meskipun terdapat beberapa kelemahan minor, kelemahan tersebut dapat diselesaikan pada aktivitas bisnis normal. Contoh karakteristik Bank yang termasuk dalam peringkat *Satisfactory* (2): a. proses identifikasi aset, ancaman, dan kerentanan memadai; b. proses pelindungan aset dilaksanakan dengan baik; c. proses deteksi insiden siber andal dan teruji; d. proses penanggulangan dan pemulihan insiden siber dilaksanakan dengan baik meskipun terdapat gangguan namun tidak bersifat signifikan.
Fair (3)	Kualitas penerapan proses ketahanan siber cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen. Contoh karakteristik Bank yang termasuk dalam peringkat *Fair* (3): a. proses identifikasi aset, ancaman, dan kerentanan cukup memadai; b. proses pelindungan aset dilaksanakan dengan cukup baik; c. proses deteksi insiden siber cukup andal dan teruji; d. proses penanggulangan dan pemulihan insiden siber dilaksanakan dengan cukup baik namun tetap menimbulkan gangguan yang bersifat minor.
Marginal (4)	Kualitas penerapan proses ketahanan siber kurang memadai. Terdapat kelemahan signifikan pada berbagai proses untuk menjaga ketahanan siber yang memerlukan tindakan korektif segera. Contoh karakteristik Bank yang termasuk dalam peringkat *Marginal* (4): a. proses identifikasi aset, ancaman, dan kerentanan kurang memadai; b. proses pelindungan aset dilaksanakan dengan kurang baik; c. proses deteksi insiden siber kurang andal dan teruji;

Peringkat	Definisi Peringkat
	d. proses penanggulangan dan pemulihan insiden siber dilaksanakan dengan kurang baik dan menimbulkan gangguan yang signifikan.
Unsatisfactory (5)	Kualitas penerapan proses ketahanan siber tidak memadai. Terdapat kelemahan signifikan pada berbagai proses untuk menjaga ketahanan siber yang tindakan penyelesaiannya di luar kemampuan manajemen. Contoh karakteristik Bank yang termasuk dalam peringkat *Unsatisfactory* (5): a. proses identifikasi aset, ancaman, dan kerentanan tidak memadai; b. proses pelindungan aset tidak dilaksanakan dengan baik; c. proses deteksi insiden siber tidak andal dan teruji; d. proses penanggulangan dan pemulihan insiden siber tidak dilaksanakan dengan baik sehingga menimbulkan gangguan yang sangat signifikan.

III.d. Matriks Penetapan Tingkat Maturitas Keamanan Siber

Peringkat	Definisi Peringkat
Tingkat 1	Mencerminkan kondisi maturitas keamanan siber Bank yang secara umum sangat tinggi, tercermin dari penerapan manajemen risiko terkait keamanan siber dan penerapan proses ketahanan siber yang secara umum sangat baik. Dalam hal terdapat kelemahan maka secara umum kelemahan tersebut tidak signifikan.
Tingkat 2	Mencerminkan kondisi maturitas keamanan siber Bank yang secara umum tinggi, tercermin dari penerapan manajemen risiko terkait keamanan siber dan penerapan proses ketahanan siber yang secara umum baik. Dalam hal terdapat kelemahan maka secara umum kelemahan tersebut kurang signifikan.
Tingkat 3	Mencerminkan kondisi maturitas keamanan siber Bank yang secara umum cukup, tercermin dari penerapan manajemen risiko terkait keamanan siber dan penerapan proses ketahanan siber yang secara umum cukup baik. Dalam hal terdapat kelemahan maka secara umum kelemahan tersebut cukup signifikan dan apabila tidak berhasil diatasi dengan baik oleh manajemen dapat mengganggu kelangsungan usaha Bank.
Tingkat 4	Mencerminkan kondisi maturitas keamanan siber Bank yang secara umum rendah, tercermin dari penerapan manajemen risiko terkait keamanan siber dan penerapan proses ketahanan siber yang secara umum kurang baik. Terdapat kelemahan yang secara umum signifikan dan tidak dapat diatasi dengan baik oleh manajemen serta mengganggu kelangsungan usaha Bank.
Tingkat 5	Mencerminkan kondisi maturitas keamanan siber Bank yang secara umum sangat rendah, tercermin dari penerapan manajemen risiko terkait keamanan siber dan penerapan proses ketahanan siber yang secara umum kurang baik. Terdapat kelemahan yang secara umum sangat signifikan sehingga untuk mengatasinya diperlukan dukungan dana dari pemegang saham atau sumber dana dari pihak lain untuk memperkuat penerapan manajemen risiko terkait keamanan siber dan penerapan proses ketahanan siber pada Bank.

Ditetapkan di Jakarta

pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN

OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum
ttd
Mufli Asmawidjaja

LAMPIRAN IV

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

IV.a. Format Notifikasi Awal Insiden Siber

NOTIFIKASI AWAL INSIDEN SIBER

A. INFORMASI BANK

1. Nama Bank : .....
2. Alamat Kantor Pusat Bank : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Otoritas/Lembaga Penerima : ..... 1)

B. INFORMASI UMUM INSIDEN SIBER

1. Tanggal dan Waktu Terjadinya Insiden Siber: 2)
   ..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
2. Tanggal dan Waktu Insiden Siber Diketahui:
   ..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
3. Jenis Insiden Siber : .....3)
4. Titik Serangan : .....4)
5. Respons Awal Bank Pasca Insiden Siber
   :..... 5)
6. Penilaian Awal atas Dampak Insiden Siber bagi Bank
   : .....6)

Keterangan:

1) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima pelaporan notifikasi awal ini (jika ada).
2) Diisi dalam hal Bank telah mengidentifikasi tanggal dan waktu terjadinya insiden siber.
3) Memuat informasi mengenai jenis insiden siber. Contoh: *malware*, *hacking*, *ransomware*, *web defacement*, *denial of services* (DoS)/*distributed denial of services* (DDoS).
4) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
5) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden siber.
6) Diisi dalam hal dampak insiden siber telah diidentifikasi (insiden siber dapat berdampak kepada antara lain produk Bank, pihak ketiga, keuangan Bank, dan reputasi Bank).

IV.b. Format Laporan Insiden Siber

LAPORAN INSIDEN SIBER

A. INFORMASI PELAPOR
1. Nama Bank : .....
2. Alamat Kantor Pusat Bank : .....
3. Nomor Telepon : .....
4. Nama Narahubung : .....
5. Nomor Telepon Narahubung : .....
6. Tanggal Penyampaian Notifikasi Awal (dd/mm/yyyy) : ..../..../.....
7. Otoritas/Lembaga Penerima : ..... 1)

B. INFORMASI UMUM INSIDEN SIBER 2)
1. Tanggal dan Waktu Terjadinya Insiden Siber: 3)
..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
2. Tanggal dan Waktu Insiden Siber Diketahui:
..../..../..... (dd/mm/yyyy), ... : .... (hh:mm)
3. Jenis Insiden Siber : ..... 4)
4. Titik Serangan : ..... 5)
5. Respons Awal Bank Pasca Insiden Siber : ..... 6)

C. PENILAIAN ATAS DAMPAK INSIDEN SIBER BAGI BANK 7)
1. Penilaian Dampak Insiden Siber terhadap Ketersediaan dan Operasional Layanan Bank 8)
.....
2. Penilaian Dampak Insiden Siber terhadap Finansial Bank 9)
.....
3. Penilaian Dampak Insiden Siber terhadap Reputasi Bank 10)
.....
4. Penilaian Dampak Insiden Siber terhadap Aspek Hukum dan Kepatuhan Bank 11)
.....
5. Penilaian Dampak Insiden Siber terhadap Pihak Ketiga 12)
.....
6. Penilaian Dampak Lainnya dari Insiden Siber yang Dapat Diidentifikasi oleh Bank
.....

D. INFORMASI KRONOLOGIS INSIDEN
1. Durasi terjadinya insiden siber.
2. Langkah eskalasi insiden siber yang dilakukan.
3. Langkah penanggulangan insiden siber yang dilakukan.
4. Langkah pemulihan insiden siber yang dilakukan.
5. Keterlibatan pihak ketiga dalam penanggulangan dan pemulihan insiden siber.
6. Pihak yang menerima informasi terkait insiden siber (pemangku kepentingan, contoh: otoritas, mitra layanan, dan nasabah).

7. Informasi pendukung yang digunakan untuk mengidentifikasi serangan siber, jika diketahui.
   (contoh: alamat IP yang mencurigakan, lalu lintas jaringan yang tidak biasa, tingkat kegagalan autentikasi yang tinggi, dan permintaan *file* secara berulang kali)

E. ANALISIS PENYEBAB TERJADINYA INSIDEN
   1. Sumber Serangan:
      a. Pihak : ..... [13)]
      b. Negara Asal : ..... [14)]
      c. Motif Serangan : ..... [15)]
   2. Faktor penyebab insiden : ..... [16)]

F. ANALISIS FINAL
   1. Kesimpulan.
   2. Langkah Perbaikan.[17)]
   3. Target Waktu Penyelesaian Insiden Siber : ..../..../.....
      (dd/mm/yy) [18)]

Keterangan:

1) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima laporan ini (jika ada).
2) Berisi informasi yang sesuai dengan informasi yang telah disampaikan pada notifikasi awal, namun dapat ditambahkan atau disesuaikan dengan informasi tambahan jika ada.
3) Diisi dalam hal Bank telah mengidentifikasi tanggal dan waktu terjadinya insiden siber.
4) Memuat informasi mengenai jenis insiden siber. Contoh: *malware*, *hacking*, *ransomware*, *web defacement*, *denial of services* (DoS)/*distributed denial of services* (DDoS).
5) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
6) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden siber.
7) Pada bagian ini informasi yang diberikan berupa penjelasan tambahan dari penilaian awal yang sudah dilakukan oleh Bank saat pelaporan notifikasi awal insiden siber.
8) Diisi dalam hal terdapat dampak terhadap bisnis Bank, termasuk dalam kaitannya dengan ketersediaan dan operasional layanan Bank. Informasi paling sedikit memuat:
   a. jenis layanan dan/atau nama produk yang terdampak (contoh: layanan *treasury*, *trade finance*, *cash management*, dan layanan perbankan digital); dan
   b. penjelasan mengenai dampak yang terjadi (jika layanan dan/atau produk yang terdampak lebih dari 1 (satu), maka penjelasan diberikan untuk seluruh layanan dan produk yang terdampak).
9) Diisi dalam hal terdapat dampak finansial dari insiden siber. Informasi paling sedikit memuat:
   a. hal yang terdampak (contoh: nilai atau volume transaksi, penarikan dana, dan likuiditas Bank); dan
   b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) hal maka penjelasan diberikan untuk seluruh hal yang terdampak).
10) Diisi dalam hal terdapat dampak terhadap reputasi Bank dari insiden siber (contoh: insiden dipublikasikan oleh media).
11) Diisi dalam hal terdapat dampak terhadap aspek hukum dan kepatuhan (contoh: pelanggaran ketentuan peraturan perundang-undangan dan adanya tuntutan hukum dari pihak terkait).
12) Diisi dalam hal terdapat dampak terhadap pihak ketiga dari Bank. Informasi paling sedikit memuat:
   a. kategori pihak ketiga (contoh: nasabah, pihak penyedia jasa, dan mitra kerja sama layanan); dan
   b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) kategori mitra maka penjelasan diberikan untuk seluruh mitra terdampak).
13) Memuat informasi mengenai pihak yang melakukan serangan atau menjadi sumber serangan, antara lain: pihak intern, pihak ekstern atau pihak ketiga (jika diketahui).
14) Memuat informasi mengenai negara asal dari sumber serangan (jika diketahui).
15) Memuat informasi mengenai motif atau tujuan atas serangan yang dilakukan oleh pelaku (jika diketahui).
16) Memuat penjelasan lengkap dari faktor yang menyebabkan terjadinya insiden siber di Bank.

17) Memuat informasi mengenai langkah yang dilakukan Bank untuk mencegah insiden serupa terjadi di masa depan.
18) Diisi dalam hal insiden belum sepenuhnya diselesaikan pada saat menyampaikan laporan kepada Otoritas Jasa Keuangan.

Ditetapkan di Jakarta
pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN V

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

Hasil Penilaian terkait Keamanan Siber Bank

Nama Bank :
Tahun :

Penilaian Risiko Inheren terkait Keamanan Siber		
No.	**Faktor Penilaian**	**Peringkat**
1.	Teknologi	
2.	Produk Bank	
3.	Karakteristik Organisasi	
4.	Rekam Jejak Insiden Siber	
Peringkat Risiko Inheren terkait Keamanan Siber		
Analisis		
Penjelasan lebih lanjut mengenai penilaian risiko inheren terkait keamanan siber pada Bank, termasuk pertimbangan Bank untuk setiap faktor penilaian sehingga memperoleh peringkat risiko inheren terkait keamanan siber.		

Penilaian Tingkat Maturitas Keamanan Siber		
No.	**Faktor Penilaian**	**Peringkat**
1.	Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber	
2.	Kualitas Penerapan Proses Ketahanan Siber	
Peringkat Tingkat Maturitas Keamanan Siber		
Analisis		
Penjelasan lebih lanjut mengenai penilaian tingkat maturitas keamanan siber pada Bank, termasuk pertimbangan Bank untuk setiap faktor penilaian sehingga memperoleh peringkat tingkat maturitas keamanan siber.		

Peringkat Tingkat Risiko terkait Keamanan Siber	

Analisis
Penjelasan lebih lanjut mengenai penetapan tingkat risiko terkait keamanan siber pada Bank, termasuk pertimbangan Bank atas peringkat risiko inheren terkait keamanan siber dan peringkat tingkat maturitas keamanan siber sehingga memperoleh tingkat risiko terkait keamanan siber.

Lampiran:
1. Kertas kerja penilaian risiko inheren terkait keamanan siber yang telah diisi oleh Bank.
2. Kertas kerja penilaian tingkat maturitas keamanan siber yang telah diisi oleh Bank.

Ditetapkan di Jakarta
pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,
ttd
DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum
ttd
Mufli Asmawidjaja

LAMPIRAN VI

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 29 /SEOJK.03/2022

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

Laporan Hasil Pengujian Keamanan Siber Berdasarkan Skenario

Nama Bank :
Tahun :

No.	Ringkasan Pelaksanaan Pengujian						Hasil Pengujian[3)]	Perbaikan yang Dilakukan[4)]	Rencana Tindak Lanjut[5)]
	Tujuan Pengujian	Jenis Pengujian[1)]	Ruang Lingkup Pengujian	Tanggal Pengujian Dimulai	Tanggal Pengujian Selesai	Pihak yang Terlibat[2)]			

Keterangan:
1) Jenis pengujian berdasarkan skenario yang dilakukan, contoh: *social engineering exercise* dan *adversarial attack simulation exercise*.
2) Pihak yang terlibat termasuk pihak penyedia jasa TI atau pihak ketiga yang digunakan oleh Bank untuk melakukan pengujian.
3) Hasil pengujian termasuk pelajaran terpetik (*lesson learned)* dan hasil observasi.
4) Perbaikan yang dilakukan dapat diisi dalam hal Bank sudah melakukan perbaikan atas hasil pengujian keamanan siber.
5) Rencana tindak lanjut diisi dalam hal Bank belum melakukan perbaikan atas hasil pengujian keamanan siber.

Ditetapkan di Jakarta
pada tanggal 27 Desember 2022

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja