Yth.

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

di tempat.

RANCANGAN

SURAT EDARAN OTORITAS JASA KEUANGAN

NOMOR ... TAHUN ...

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 suatu Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Pesatnya perkembangan Teknologi Informasi (TI) telah mempengaruhi 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 mudah bagi nasabah. Namun demikian, peningkatan pemanfaatan TI juga berpotensi meningkatkan risiko 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 perlu untuk 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-langkah yang tepat sasaran, dan berkelanjutan dalam mengatasi permasalahan siber. Hal tersebut harus dilakukan mengingat bisnis perbankan merupakan bisnis yang berkaitan dengan dana masyarakat yang memerlukan operasional yang matang dan aman.

2. Ketahanan siber merupakan kemampuan Bank untuk tetap menjaga kelangsungan bisnisnya dengan melakukan tindakan antisipatif dan adaptif terhadap ancaman siber.
3. Keamanan siber merupakan kondisi terjaganya kerahasiaan, keutuhan, dan 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.

II. PENILAIAN RISIKO INHEREN TERKAIT KEAMANAN SIBER

1. Bank melakukan penilaian atas risiko inheren terkait keamanan siber. Penilaian tersebut dilakukan secara tahunan untuk posisi akhir bulan Desember. Bank dapat melakukan pengkinian penilaian tersebut sewaktu-waktu apabila diperlukan.
2. Penilaian risiko inheren terkait dengan keamanan siber dilakukan dengan memperhatikan paling sedikit 4 (empat) faktor penilaian, yaitu teknologi, produk bank, karakteristik organisasi, serta rekam jejak insiden siber. Penilaian risiko inheren diawali dari penilaian terhadap parameter risiko pada setiap faktor risiko terkait keamanan siber. Terdapat beberapa parameter atau indikator minimum yang dapat dijadikan acuan oleh Bank dalam menilai risiko inheren terkait keamanan siber, dengan berpedoman pada 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. 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*), dengan

berpedoman pada Lampiran III.a yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

4. Dalam melakukan penilaian sendiri atas risiko inheren terkait keamanan siber, Bank menggunakan format sebagaimana pada Lampiran II.a yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
5. Hasil penilaian risiko inheren terkait keamanan siber disampaikan kepada Otoritas Jasa Keuangan dengan menggunakan format pada Lampiran V yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

III. PENERAPAN MANAJEMEN RISIKO TERKAIT KEAMANAN SIBER

1. Bank menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI sebagaimana diatur dalam Pasal 15 ayat (1) POJK PTI. Manajemen risiko berlaku untuk seluruh penyelenggaraan TI, termasuk terkait keamanan siber.
2. Penerapan manajemen risiko terkait keamanan siber mencakup 4 (empat) aspek, yaitu:
   a. Tata kelola, yang meliputi pengawasan aktif direksi dan dewan komisaris, sumber daya manusia, struktur organisasi, serta budaya dan kesadaran;
   b. Kerangka manajemen risiko terkait keamanan siber, yang meliputi penetapan tingkat risiko yang akan diambil dan toleransi risiko, strategi manajemen risiko, serta penetapan kebijakan, prosedur, dan limit;
   c. Proses manajemen risiko terkait keamanan siber, yang meliputi identifikasi risiko, pengukuran risiko, pemantauan risiko, dan pengendalian risiko, serta sistem informasi manajemen risiko terkait keamanan siber; dan
   d. Sistem pengendalian intern.
3. Penerapan manajemen risiko terkait keamanan siber disesuaikan dengan karakteristik dan kompleksitas bisnis serta TI yang digunakan.

IV. PENERAPAN PROSES KETAHANAN SIBER BAGI BANK UMUM

1. Sebagaimana diatur dalam Pasal 21 POJK PTI, Bank menjaga ketahanan siber dengan melakukan proses paling sedikit:
   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:

   a. menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, sumber daya manusia, jaringan, dan infrastruktur) dan pencatatan konfigurasi secara efektif;
   b. melakukan *vulnerability assessment* dan pemantauan terhadap perkembangan siber terkini untuk mengidentifikasi ancaman siber;
   c. melakukan pengujian keamanan siber secara berkala.

3. Proses Pelindungan Aset

   Pada proses pelindungan aset, Bank:

   a. menerapkan pengendalian keamanan (*security control*) yang komprehensif sesuai dengan hasil identifikasi sebagaimana pada angka 2, yang bertujuan untuk memastikan:
      1) keberlangsungan dan ketersediaan sistem informasi;
      2) integritas, kerahasiaan, serta ketersediaan data dan informasi; dan
      3) kesesuaian dengan ketentuan peraturan perundang-undangan dan standar yang berlaku.
   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 dengan kebijakan dan prosedur yang berlaku.
   d. memperbarui pengendalian keamanan Bank secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan sesuai dengan proses identifikasi terkini.
   e. menerapkan manajemen keamanan data dan informasi serta memastikan bahwa data dan/atau informasi dikelola sesuai dengan strategi risiko organisasi untuk melindungi kerahasiaan, integritas, dan ketersediaan data serta 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, infrastuktur jaringan, dan komponen sistem yang dikelola oleh Bank.
   h. menerapkan pelindungan yang memadai dalam penggunaan *cloud computing* sesuai dengan layanan yang digunakan (antara lain *Software-as-a-service* (SaaS), *Platform-as-a-service* (PaaS), dan

Infrastructure-as-a-service (IaaS)), dalam hal Bank menggunakan *cloud computing*.

i. memastikan penerapan *secure coding* dalam pengembangan sistem dan aplikasi untuk memastikan integritas sistem dan aplikasi.

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:

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

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

c. memastikan ketersediaan proses untuk mendeteksi insiden siber secara memadai.

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

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:

a. memastikan ketersediaan rencana penanggulangan dan pemulihan saat insiden siber terjadi untuk memastikan penanggulangan yang tepat waktu dalam mengembalikan layanan secepat mungkin 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 suatu insiden menjadi berkembang dengan memitigasi efek dan menanggulangi insiden tersebut.

d. melakukan analisis untuk memastikan langkah penanggulangan dan pemulihan insiden siber dijalankan dengan tepat.

e. menerapkan eskalasi dan pelaporan atas insiden siber.

V. PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

1. Penilaian maturitas keamanan siber bertujuan untuk menentukan tingkat maturitas yang telah dicapai oleh Bank serta mengidentifikasi kesenjangan dan area yang memerlukan perbaikan terhadap penerapan manajemen risiko terkait keamanan siber dan proses menjaga ketahanan siber Bank. Area yang teridentifikasi untuk diperbaiki dapat menjadi masukan dalam penyusunan *roadmap* untuk meningkatkan ketahanan dan keamanan siber Bank.

2. Tata Cara Penilaian Tingkat Maturitas Keamanan Siber

a. Bank melakukan penilaian sendiri atas tingkat maturitas keamanan siber. Penilaian tersebut dilakukan secara tahunan untuk posisi akhir bulan Desember. Bank dapat melakukan pengkinian 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 tata kelola, kerangka manajemen risiko, proses manajemen risiko dan sistem informasi manajemen risiko, serta kecukupan sistem pengendalian risiko; dan

2) kualitas penerapan proses ketahanan siber, yang meliputi proses identifikasi aset, ancaman, dan kerentanan, proses pelindungan aset, proses deteksi insiden siber, serta proses penanggulangan dan pemulihan insiden siber.

c. Dalam menilai 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 dimaksud pada Lampiran I.b dan Lampiran I.c yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

d. 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*), dengan berpedoman pada:

1) Lampiran III.b yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini, bagi penerapan manajemen risiko terkait keamanan siber.

2) Lampiran III.c yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini, bagi penerapan proses ketahanan siber.

e. Penetapan tingkat maturitas keamanan siber dikategorikan dalam 5 (lima) tingkat, yaitu Tingkat 1, Tingkat 2, Tingkat 3, Tingkat 4, dan Tingkat 5, dengan berpedoman pada Lampiran III.d yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

f. Dalam melakukan penilaian sendiri atas tingkat maturitas keamanan siber, Bank menggunakan format sebagaimana pada Lampiran II.b yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

3. Penyampaian Hasil Penilaian Sendiri atas Tingkat Maturitas Keamanan Siber

Hasil penilaian sendiri atas tingkat maturitas keamanan siber sebagaimana dimaksud pada angka 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 dengan menggunakan format pada Lampiran V yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

4. Pelaksanaan dan Penyampaian Hasil Penilaian Sendiri atas Tingkat Maturitas Keamanan Siber untuk Pertama Kali

Penilaian sendiri atas 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 verifikasi atas hasil penilaian tingkat maturitas keamanan siber sebagaimana dimaksud pada angka 3. Dalam rangka pengawasan Bank, apabila berdasarkan verifikasi Otoritas Jasa Keuangan menunjukkan bahwa hasil penilaian maturitas keamanan siber tidak mencerminkan kondisi Bank yang sebenarnya, Otoritas Jasa Keuangan dapat menyesuaikan hasil penilaian tingkat maturitas keamanan siber.

VI. TINGKAT RISIKO TERKAIT KEAMANAN SIBER

1. Tingkat risiko terkait keamanan siber ditetapkan berdasarkan penilaian atas tingkat risiko inheren terkait keamanan siber dan tingkat maturitas keamanan siber. Tingkat risiko terkait keamanan siber ditetapkan paling

tinggi sebesar risiko inheren terkait keamanan siber sebagaimana dimaksud dalam Butir II.

Contoh: Risiko inheren terkait keamanan siber Bank A ditetapkan Peringkat 3 (*moderate*). Tingkat maturitas keamanan siber Bank A ditetapkan Tingkat 4. Bank A dalam menetapkan tingkat risiko terkait keamanan siber paling tinggi sebesar Tingkat Risiko 3.

2. Tingkat risiko terkait keamanan siber dapat dipertimbangkan sebagai parameter atau indikator tambahan dari tingkat risiko operasional dalam penilaian tingkat kesehatan Bank, terutama bagi Bank yang memanfaatkan TI secara signifikan.
3. Hasil penilaian tingkat risiko terkait keamanan siber disampaikan kepada Otoritas Jasa Keuangan dengan menggunakan format pada Lampiran V yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

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, adanya perubahan yang material pada sistem elektronik atau arsitektur TI pada bank, dan adanya peningkatan eksposur risiko terkait keamanan siber. Pengujian ini diawali dengan pelaksanaan identifikasi kerentanan (*vulnerability assessment)* yang kemudian dilanjutkan dengan *penetration testing*.

   Penetration testing 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 testing* bertujuan untuk menerobos sistem pengamanan yang ada, sesuai dengan batasan yang telah ditentukan sebelumnya. Selanjutnya, *penetration testing* 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 *online*.

3. Pengujian Keamanan Siber Berdasarkan Skenario

Pengujian keamanan siber berdasarkan skenario perlu dilakukan oleh Bank untuk memvalidasi proses penanggulangan dan pemulihan Bank, serta rencana komunikasi Bank, dalam menghadapi ancaman siber. Dalam pelaksanaan pengujian ini, Bank harus melibatkan *stakeholders* yang relevan, termasuk manajemen senior, 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, adversarial attack simulation exercise,* dan/atau pengujian lainnya.

a. *Table-top Exercise*

Table-top exercise adalah suatu kegiatan berbasis diskusi dimana sumber daya manusia 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 adalah pengujian yang menggunakan representasi simulasi yang interaktif dari 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 adalah pengujian dengan menggunakan skenario dimana penyerang memanipulasi individu yang kurang waspada untuk membocorkan informasi sensitif seperti kata sandi, melalui penggunaan teknik seperti *phising* dan *spam*. Pengujian ini dapat dilakukan untuk mengetahui tingkat kesadaran keamanan siber dari pegawai.

d. *Adversarial Attack Simulation Exercise*

Adversarial Attack Simulation Exercise (AASE) adalah pengujian yang menggunakan simulasi taktik, teknik, dan prosedur dari serangan siber di dunia nyata untuk menargetkan sumber daya manusia, 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.

Adapun beberapa 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.
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 internal, peningkatan kapasitas, kesadaran Bank terhadap keamanan siber, serta proses ketahanan 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 testing* di tahun 2022, antara lain pada bulan Maret 2022, Juli 2022, dan November 2022. Kompilasi hasil pengujian

keamanan siber berupa *penetration testing* 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 dilaksanakan. Pengujian keamanan siber selesai dilaksanakan pada saat laporan hasil pengujian selesai disusun.

Hasil pengujian keamanan siber paling sedikit mencakup:

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 Oktober 2022. Selanjutnya, pengujian tersebut selesai dilakukan dan laporan hasil pengujian telah selesai disusun pada tanggal 14 Oktober 2022. Hasil pengujian keamanan siber tersebut disampaikan kepada Otoritas Jasa Keuangan paling lambat pada tanggal 28 Oktober 2022.

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 pada Butir IV;
   b. penilaian sendiri atas tingkat maturitas keamanan siber; dan
   c. pengujian keamanan siber.
3. Unit atau fungsi yang menangani ketahanan dan keamanan siber Bank bersifat independen terhadap fungsi pengelolaan TI yang 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 respon 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 kerja atau fungsi terkait (antara lain spesialis keamanan teknis, unit bisnis, fungsi legal, sumber daya manusia, dan tim komunikasi eksternal) dan mampu mengakses informasi yang diperlukan dengan cepat (misalnya informasi dari penyedia jasa pihak ketiga atau informasi pendukung lainnya);

c. tim tanggap insiden siber memiliki sumber daya analisis insiden (misalnya daftar *host, packet sniffer*, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat *digital forensic*, dan sumber daya lain yang diperlukan); dan

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

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

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 *website* dengan cara mengganti atau memodifikasi *website* sehingga isi dari *website* berubah sesuai dengan keinginan penyerang.

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

DoS dan DDoS merupakan serangan yang bertujuan untuk mengganggu *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. Sebagai bentuk komunikasi kepada para pemangku kepentingan dan pengendalian atas pengelolaan ketahanan dan keamanan siber, Bank perlu melakukan pemantauan atas insiden siber. Kegiatan pemantauan insiden siber dapat bermanfaat bagi Bank dalam melakukan penanggulangan dan pemulihan terhadap sistem elektronik Bank, sehingga 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 disampaikan oleh Bank dengan ketentuan sebagai berikut:
   a. notifikasi awal disusun dengan menggunakan format sebagaimana dimaksud pada 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, yang 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 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 dengan menggunakan format sebagaimana dimaksud pada 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. Bank menyampaikan laporan insiden siber melalui sistem pelaporan Otoritas Jasa Keuangan dengan alamat https://sipena.ojk.go.id/ atau alamat lain yang ditetapkan Otoritas Jasa Keuangan.
8. 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. Apabila 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	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 2022 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 ketentuan Otoritas Jasa Keuangan, 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 2022 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 ketentuan Otoritas Jasa Keuangan.

Contoh:

Ketentuan Otoritas “C”

Jangka waktu penyampaian notifikasi awal	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 2022 pukul 13.00 WITA. Mengingat jangka waktu penyampaian notifikasi awal dan/atau laporan insiden siber berdasarkan ketentuan Otoritas Jasa Keuangan 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 dalam kurun waktu 5 (lima) hari kerja setelah insiden siber diketahui kepada Otoritas Jasa Keuangan.

X. PENUTUP

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

Ditetapkan di Jakarta
pada tanggal ...

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN,

DIAN EDIANA RAE

LAMPIRAN I

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR …

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	Interkoneksi ke internet publik	Jumlah interkoneksi Bank ke internet publik mempengaruhi risiko inheren Bank. Semakin banyak jumlah interkoneksi maka semakin besar risiko inheren Bank.
		Interkoneksi ke pihak ketiga (*third party*)	Terdapat beberapa tipe koneksi dari Bank ke pihak ketiga, yaitu: 1) *Direct connection* (*clear channel*/*link*/MLPLS/*IP Based*) (*Open System Interconnection* (OSI) *Layer* 3) 2) *Host to Host* - FTP/SFTP (OSI *Layer* 4) 3) *Application Programming Interface*/API (OSI *Layer* 7) Penggunaan tipe koneksi mempengaruhi risiko inheren Bank. Semakin banyak koneksi yang menggunakan *direct connection* maka semakin besar risiko inheren Bank.
		Akses ke aset teknologi informasi (TI) internal Bank	Akses ke aset TI internal 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 internal Bank serta metode yang digunakan mempengaruhi risiko inheren Bank. Semakin banyak pihak yang dapat mengakses aset TI internal Bank maka semakin besar risiko inheren Bank.
		Jaringan Intranet dari kantor cabang	Akses langsung dari jaringan kantor ke *core system*/aset TI internal melalui intranet mempengaruhi risiko inheren Bank. Semakin banyak jumlah kantor cabang yang memiliki akses ke *core system* maka semakin besar risiko inheren Bank.
		Penggunaan jasa *cloud service provider*	Penggunaan jasa *cloud service provider* dapat dibagi menjadi beberapa tingkatan, yaitu: 1) untuk *collaboration tools*; 2) untuk *platform* TI; dan/atau 3) untuk infrastruktur TI. Semakin Bank bergantung pada *cloud service* maka semakin besar risiko inheren Bank. Selain itu penyimpanan atau pemrosesan data transaksional dalam layanan yang menggunakan jasa *cloud service provider* mengakibatkan risiko inheren yang tinggi pada Bank.
		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 unit atau fungsi pada Bank dan/atau menggunakan pihak ketiga. Semakin Bank bergantung pada pihak ketiga dalam

No.	Parameter atau Indikator		Keterangan
			pengelolaan perangkat lunak yang digunakan untuk mendukung kegiatan operasional Bank maka semakin besar risiko inheren Bank.
		Penggunaan perangkat keras dan/atau perangkat lunak yang sudah dan/atau akan masuk masa *End-of-life* (EOL)	Penggunaan perangkat keras dan/atau perangkat lunak yang sudah masuk masa EOL mempengaruhi risiko inheren Bank. Semakin banyak Bank menggunakan perangkat keras dan/atau perangkat lunak yang sudah masuk/mendekati masa EOL maka semakin besar risiko inheren Bank.
		Jumlah Pegawai yang dapat memiliki akses koneksi perangkat pribadi ke jaringan Bank (kebijakan *Bring Your Own Device*/BYOD)	Kebijakan BYOD dapat dilihat dari 2 (dua) sisi, yaitu jumlah pegawai yang diperbolehkan mengakses jaringan Bank melalui perangkat pribadi dan jenis perangkat yang diperbolehkan untuk mengakses. Semakin banyak pegawai dan jenis perangkat yang diperbolehkan maka semakin besar risiko inheren Bank.
		Perangkat lunak yang dapat diakses menggunakan perangkat pribadi ke jaringan Bank (kebijakan *Bring Your Own Device*/BYOD)	Perangkat lunak internal Bank yang dapat diakses oleh perangkat pribadi terbagi menjadi 3 (tiga), yaitu: 1) Aplikasi email; 2) Aplikasi penunjang; 3) Aplikasi kritikal; dan 4) *Core banking system.* Semakin tinggi kritikalitas aplikasi yang dapat diakses oleh perangkat pribadi maka semakin besar risiko inheren Bank.
		Pihak ketiga yang memiliki akses terhadap sistem internal Bank dan/atau informasi sensitif	Pihak ketiga dalam hal ini termasuk perusahaan (eksternal dan *intragroup*) dan individu dari vendor dan/atau subkontraktor. Jumlah pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif Bank mempengaruhi risiko inheren Bank. Semakin banyak pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif Bank maka semakin besar risiko inheren Bank
2	Produk Bank	Penggunaan Saluran *Online* dan *Mobile* dalam memberikan layanan	Saluran *online* dan *mobile* dapat digunakan oleh Bank untuk: 1) penyampaian informasi umum Bank kepada masyarakat (a.l. lokasi kantor cabang, produk Bank yang tersedia, dsb.) 2) pelayanan transaksi perbankan (produk Bank); dan/atau 3) interkoneksi dengan ekosistem ekonomi digital (*super app*). Semakin luas penggunaan saluran *online* dan *mobile* yang dimiliki Bank maka semakin besar risiko inheren Bank.
		Mekanisme pengelolaan *automated teller machine* (ATM)	Pengelolaan ATM Bank dapat dilakukan sendiri oleh Bank atau menggunakan pihak ketiga, atau kombinasi keduanya. Semakin besar peran internal Bank pengelolaan ATM maka semakin besar risiko inheren Bank.

No.	Parameter atau Indikator		Keterangan
		Produk Bank berupa alat pembayaran menggunakan kartu (kartu debit, kartu kredit, dan/atau *prepaid card*)	Produk Bank berupa kartu debit dan/atau kartu kredit mempengaruhi risiko inheren Bank. Bank yang memiliki produk kartu debit dan kartu kredit memiliki risiko inheren yang lebih besar dibandingkan dengan Bank yang hanya memiliki produk kartu debit atau Bank yang tidak memiliki kedua produk tersebut.
		Jenis Produk Bank Berbasis TI	Jenis produk Bank yang berbasis TI mempengaruhi risiko inheren Bank. Semakin banyak jenis produk Bank yang berbasis TI maka semakin besar risiko inheren Bank.
		Bank sebagai penyedia jasa TI	Penyediaan jasa TI oleh Bank mempengaruhi risiko inheren Bank. Semakin banyak Bank memberikan jasa TI kepada pihak lain maka semakin besar risiko inheren Bank.
3	Karakteristik Organisasi	Organisasi Keamanan Siber	Integrasi peran dan tanggung jawab keamanan siber pada Bank mempengaruhi risiko inheren Bank. Semakin terintegrasinya peran dan tanggung jawab keamanan siber dengan layanan TI yang tersedia maka semakin rendah risiko inheren Bank.
		Posisi/Jabatan Keamanan Siber	Ketersediaan sumber daya manusia pada posisi manajerial terkait dengan keamanan siber mempengaruhi risiko inheren Bank. Semakin sering terdapat kekosongan pada posisi manajerial terkait dengan keamanan siber maka semakin besar risiko inheren Bank.
		Perubahan (*turnover*) pada SDM di TI/Keamanan Siber	Perubahan pada SDM di TI/Keamanan Siber mempengaruhi risiko inheren Bank. Semakin sering terjadi pergantian sumber daya manusia maka semakin besar risiko inheren Bank.
		Perubahan di lingkungan TI	Perubahan di lingkungan TI tercermin dari implementasi sistem dengan risiko tinggi yang ada pada Bank. Semakin banyak Bank mengimplementasikan sistem dengan risiko tinggi maka semakin besar risiko inheren Bank.
		Pengelolaan *privilege access* (administrator dan selevel administrator) di seluruh perangkat (*host*, jaringan, *database*, aplikasi, dan *cloud*)	Pengelolaan *privilege access* pada perangkat Bank mempengaruhi risiko inheren Bank. Semakin banyak tipe perangkat yang dikelola oleh pihak selain unit TI maka semakin besar risiko inheren Bank.
4	Rekam Jejak Insiden Siber	Jumlah Insiden Siber dalam 12 bulan terakhir	Jumlah insiden siber mempengaruhi risiko inheren Bank. Semakin banyak insiden siber yang berdampak signifikan maka semakin besar risiko inheren Bank.

I.b Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber

Matriks Parameter atau Indikator Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber

No.	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
1	Tata Kelola	Pengawasan Aktif Direksi dan Dewan Komisaris	Bank menetapkan wewenang dan tanggung jawab Dewan Komisaris terkait dengan penerapan manajemen risiko terkait keamanan siber.	Wewenang dan tanggung jawab Dewan Komisaris paling sedikit meliputi: 1) Memiliki tanggung jawab penuh atas penerapan manajemen risiko terkait keamanan siber Bank; 2) Bertanggung jawab untuk 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 sumber daya manusia 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 terhadap risiko siber bagi pegawai dan seluruh elemen organisasi Bank; 7) Melakukan pengawasan secara aktif atas penerapan manajemen risiko terkait keamanan siber; 8) Menyetujui kebijakan dan rencana strategis terkait manajemen risiko terkait keamanan siber yang ditetapkan sesuai dengan tingkat risiko yang akan diambil dan toleransi risiko Bank; 9) 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-faktor yang mempengaruhi kegiatan usaha Bank secara signifikan; 10) Mengevaluasi pertanggungjawaban Direksi dan memberikan arahan perbaikan atas pelaksanaan kebijakan manajemen risiko terkait keamanan siber secara berkala; dan 11) Memastikan kebijakan dan proses manajemen risiko terkait keamanan siber dilaksanakan secara efektif dan terintegrasi dalam proses manajemen risiko secara keseluruhan.

			Bank menetapkan wewenang dan tanggung jawab Direksi terkait dengan penerapan manajemen risiko terkait keamanan siber.	Wewenang dan tanggung jawab Direksi paling sedikit meliputi: 1) Memiliki tanggung jawab penuh atas penerapan manajemen risiko terkait keamanan siber Bank; 2) Bertanggung jawab untuk 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 sumber daya manusia 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 terhadap risiko 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 mengkinikan prosedur untuk mengidentifikasi, mengukur, memonitor, dan mengendalikan risiko 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 terkait keamanan siber, satuan kerja manajemen risiko, satuan kerja kepatuhan, dan satuan kerja audit internal; 11) Mengevaluasi dan/atau mengkinikan kebijakan, strategi, dan kerangka manajemen risiko operasional dan 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 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 atau manajemen senior yang memiliki keterampilan, pengetahuan, dan pengalaman yang sesuai untuk bertanggung jawab atas strategi keamanan siber Bank yang memimpin unit kerja atau 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 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 terkait risiko terkait keamanan siber yang material disertai dengan langkah-langkah perbaikan yang telah, sedang, dan akan dilakukan; 18) Memastikan pelaksanaan langkah-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 meninjau dan menyetujui seluruh perubahan konfigurasi yang dilakukan dalam sistem Bank melalui *Change Management System* yang dikaji ulang secara berkala; dan 21) Memastikan kaji ulang terhadap rencana penanganan penanggulangan dan pemulihan insiden siber Bank dilaksanakan secara berkala.
		Sumber Daya Manusia	Direksi memastikan kecukupan kuantitas dan kualitas sumber daya manusia yang ada di Bank dan memastikan sumber daya manusia	

			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.	
			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.	
			Direksi memastikan bahwa seluruh sumber daya manusia memiliki pemahaman yang memadai atas risiko terkait keamanan siber dan mampu mengomunikasikan implikasi risiko terkait keamanan siber kepada Dewan Komisaris, Direksi, manajemen, dan nasabah.	
			Direksi memastikan agar seluruh sumber daya manusia memahami strategi, tingkat risiko terkait keamanan siber yang akan diambil dan toleransi risiko terkait keamanan siber, kerangka manajemen risiko terkait keamanan siber yang telah ditetapkan oleh Direksi dan disetujui oleh Dewan Komisaris, serta memastikan seluruh sumber daya manusia menerapkan secara konsisten dalam aktivitas yang ditangani.	
			Bank memiliki informasi yang utuh mengenai seluruh pengawai 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 karyawan baru, dalam rangka melindungi *stakeholder* maupun reputasi Bank, serta mencegah potensi terjadinya aktivitas kriminal.
			Bank mengembangkan dan mengimplementasikan program berkelanjutan untuk peningkatan kapasitas terkait keamanan	Program peningkatan kapasitas dapat berupa: 1) identifikasi ancaman siber saat ini termasuk berbagai bentuk serangan *social engineering*, antara lain *phishing*, *scam phone*, dan *impersonation call*;

			siber kepada seluruh pegawai di semua tingkatan, termasuk level Dewan Komisaris, Direksi, dan manajemen untuk memastikan bahwa setiap pegawai memiliki kompetensi dan keahlian untuk menjalankan peran dan tanggung jawab secara efektif.	2) taktik serangan siber; 3) pengamanan termasuk penggunaan *secure authentication* dan cara mengidentifikasi dan melindungi, menyimpan, mengirimkan, mengarsipkan, dan memusnahkan informasi sensitif dengan benar; 4) penyebab kebocoran data secara tidak sengaja, seperti kehilangan perangkat seluler karyawan atau ketidaksengajaan mengirim *email* ke orang yang salah; 5) pelindungan data, pembatasan penggunaan, dan dokumentasi proses penanganan data sensitif *stakeholder*; 6) kewajiban menjaga data pribadi dan pengungkapan data sesuai dengan ketentuan peraturan perundang-undangan; 7) penerapan *secure code* yang baik dalam pengembangan perangkat lunak; dan/atau 8) praktik respons insiden yang tepat. Adapun frekuensi dan substansi peningkatan kapasitas disesuaikan dengan peran dan tanggung jawab masing-masing pegawai.
			Bank melakukan analisis kesenjangan (*gap analysis*) untuk memahami tingkat pengetahuan dan kemampuan pegawai terkait keamanan siber dan menggunakan informasi tersebut untuk membuat rencana aksi peningkatan kapasitas pegawai.	Dalam melakukan peningkatan kapasitas pegawai Bank dapat mengacu pada ketentuan peraturan perundang-undangan mengenai pelindungan infrastruktur informasi vital beserta ketentuan turunannya yang terkait. Salah satu contoh peningkatan kapasitas pengawai antara lain pendidikan dan pelatihan terkait keamanan siber paling sedikit 2 (dua) kali dalam setahun.
		Struktur Organisasi	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.	
			Struktur organisasi dirancang untuk memastikan bahwa satuan kerja yang melakukan fungsi pengendalian intern terhadap manajemen risiko terkait keamanan siber independen terhadap satuan kerja bisnis.	
			Bank memastikan satuan kerja manajemen risiko memiliki fungsi yang menangani	Wewenang dan tanggung jawab fungsi yang menangani penerapan manajemen risiko terkait keamanan siber, yaitu:

			penerapan manajemen risiko terkait keamanan siber.	a. memberikan masukan kepada Direksi dalam penyusunan kebijakan, strategi, dan kerangka manajemen risiko terkait keamanan siber; b. mengembangkan prosedur dan alat untuk penerapan kontrol keamanan siber; c. mendesain dan menerapkan perangkat yang dibutuhkan dalam penerapan kontrol keamanan siber; d. memantau implementasi kebijakan, strategi, dan kerangka manajemen risiko terkait keamanan siber yang ditetapkan oleh Direksi dan telah disetujui oleh Dewan Komisaris; e. melakukan pengujian ketahanan siber guna mengetahui dampak dari implementasi kebijakan dan strategi manajemen risiko terkait keamanan siber terhadap profil risiko Bank secara keseluruhan; f. mengkaji usulan produk baru dan penggunaan teknologi baru yang dikembangkan oleh suatu unit tertentu Bank yang difokuskan terutama pada dampak dari produk baru dan penggunaan terknologi baru tersebut terhadap eksposur risiko terkait keamanan siber Bank secara keseluruhan; dan g. memberikan rekomendasi kepada Direksi dan/atau satuan kerja terkait penerapan manajemen risiko terkait keamanan siber.
			Bank memiliki unit kerja atau fungsi yang bertugas menangani ketahanan dan keamanan siber.	Struktur unit kerja atau fungsi yang bertugas menangani ketahanan dan keamanan siber disesuaikan dengan ukuran dan kompleksitas kegiatan usaha Bank serta risiko keamanan siber Bank.
		Budaya dan Kesadaran	Direksi mengembangkan budaya bahwa seluruh pegawai di semua level memiliki tanggung jawab penting dalam memastikan terciptanya keamanan siber.	Budaya ini disampaikan melalui komunikasi yang jelas dan efektif serta mencakup informasi yang relevan tentang strategi keamanan siber kepada seluruh pegawai.
			Direksi membangun dan memelihara kesadaran dan komitmen yang kuat terhadap keamanan siber Bank.	Hal ini dapat dilakukan antara lain dengan program peningkatan kesadaran 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.
			Bank memastikan bahwa seluruh pegawai dan *stakeholders* terkait memahami dan menerapkan kebijakan keamanan siber secara efektif	Salah satu cara memverifikasi pemahaman kesadaran keamanan siber adalah dengan melakukan simulasi *phishing* dengan cara mengirimkan email *blast* kepada seluruh pegawai untuk mengukur respons terhadap *phishing* dan serangan email serupa setidaknya sekali setiap tahun.

2	Kerangka Manajemen Risiko terkait Keamanan Siber	Penetapan Tingkat Risiko yang Akan Diambil dan Toleransi Risiko Terkait Keamanan Siber	Direksi bertanggung jawab untuk menetapkan tingkat risiko yang diambil terkait keamanan siber Bank.	Tingkat risiko yang akan diambil merupakan tingkat yang bersedia diambil oleh Bank dalam rangka mencapai sasaran tingkat maturitas penerapan manajemen risiko terkait keamanan siber Bank. Tingkat risiko yang akan diambil tercermin dalam strategi dan sasaran manajemen risiko terkait keamanan siber Bank secara keseluruhan. Toleransi risiko terkait dengan 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 diambil dan toleransi risiko terkait keamanan siber, Direksi harus memperhatikan strategi, tujuan, dan kemampuan Bank dalam mengambil risiko (*risk bearing capacity*).
			Direksi bertanggung jawab untuk menetapkan toleransi risiko terkait keamanan siber Bank.	
		Strategi Manajemen Risiko Terkait Keamanan Siber	Bank harus 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 dan toleransi risiko 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 antara lain: 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 terbaru, kecukupan sumber daya manusia dan infrastruktur pendukung, karakteristik dan kompleksitas kegiatan usaha, serta kondisi keuangan Bank.
			Bank memastikan bahwa seluruh peran dan tanggung jawab terkait keamanan siber didefinisikan dengan jelas dalam strategi manajemen risiko terkait keamanan siber.	Strategi manajemen risiko terkait keamanan siber Bank paling sedikit harus 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, dan 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-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 keamanan 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 oleh insiden siber dan pelanggaran keamanan siber.
			Direksi mengomunikasikan strategi manajemen risiko terkait keamanan siber secara efektif kepada seluruh satuan kerja dan pegawai agar dipahami secara jelas.	
			Direksi melakukan kaji ulang strategi manajemen risiko terkait keamanan siber secara berkala untuk menentukan apakah perlu dilakukan perubahan terhadap strategi manajemen risiko tersebut.	
		Penetapan Kebijakan, Prosedur, dan Limit	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.
			Bank mendesain dan mengimplementasikan kebijakan dan prosedur dengan memperhatikan karakteristik dan kompleksitas kegiatan usaha, tingkat risiko yang akan diambil dan toleransi risiko, profil risiko, serta peraturan yang ditetapkan otoritas terkait dengan keamanan siber.	
			Bank melakukan internalisasi kebijakan manajemen risiko terkait keamanan siber termasuk strategi dan tujuan manajemen risiko terkait keamanan siber ke dalam proses bisnis seluruh lini bisnis dan aktivitas pendukung, termasuk kebijakan yang bersifat spesifik	

			sesuai dengan kebutuhan lini bisnis dan aktivitas pendukung Bank.	
			Kebijakan manajamen risiko terkait keamanan siber secara umum harus memenuhi beberapa hal.	Hal-hal yang harus dipenuhi, antara lain: 1) memuat bagaimana Bank menetapkan toleransi risiko terkait keamanan siber dan tata cara Bank mengidentifikasi, mengurangi, dan mengelola risiko terkait keamanan siber; 2) memuat rencana kelangsungan usaha (*business continuity plan*) atas kemungkinan kondisi ekstern dan intern terburuk dari serangan siber, antara lain melalui pelaksanaan *business impact analysis*; 3) disusun dengan menggunakan standar dan pedoman yang berlaku secara nasional maupun internasional sebagai bahan perbandingan; 4) konsisten dengan kerangka manajemen risiko Bank secara keseluruhan; 5) memuat hal yang spesifik terkait dengan keamanan siber, antara lain: a) Pelindungan data; b) Kepatuhan sumber daya manusia terhadap kebijakan manajemen risiko terkait keamanan siber termasuk sanksi yang dikenakan apabila terjadi pelanggaran; c) Keamanan informasi termasuk pengaturan mengenai otentikasi antara lain melalui *single* ID yang unik dan pengaturan tenggat waktu kadaluarsa hak akses akun pengguna, serta prosedur penambahan/perubahan/ penghapusan hak akses dalam hal terjadi perpindahan karyawan; d) Metode pelaporan dari karyawan dan nasabah terkait kehilangan perangkat keras maupun perangkat lunak yang memungkinkan untuk digunakan sebagai sarana untuk melakukan ancaman keamanan siber; e) Metode manajemen data termasuk namun tidak terbatas pada pelindungan data, transfer data, dan penghapusan data; f) Metode pengendalian kriptografi; g) Kepatuhan terhadap ketentuan peraturan perundang-undangan mengenai hak kekayaan intelektual; h) Metode verifikasi integritas dan pengujian terhadap perangkat keras dan perangkat lunak yang diperoleh dari luar Bank; dan i) 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.

			Bank memiliki prosedur yang merupakan turunan dari kebijakan manajemen risiko terkait keamanan siber, yang dapat berupa pengendalian operasional yang bersifat umum pada seluruh lini bisnis dan aktivitas pendukung Bank dan kontrol operasional yang bersifat spesifik pada masing-masing lini bisnis dan aktivitas pendukung Bank.	
			Bank memiliki proses, prosedur, dan kebijakan keamanan siber (mengatur tujuan, cakupan, fungsi, tanggung jawab, komitmen manajemen, dan koordinasi antar entitas organisasi) yang dikelola dan digunakan untuk mengatur pelindungan sistem informasi dan aset.	
			Bank memiliki proses, prosedur, dan kebijakan manajemen risiko terkait keamanan untuk pihak ketiga (termasuk subkontrak) yang mengatur tentang pengelolaan termasuk pemrosesan dan penghapusan data/informasi digital milik Bank (termasuk data nasabah yang dimiliki Bank) oleh pihak ketiga.	Proses, prosedur, dan kebijakan manajemen risiko terkait keamanan siber untuk pihak ketiga antara lain: 1) Proses untuk memblokir upaya akses perangkat milik karyawan dan perangkat pihak ketiga yang tidak aman; 2) Validasi dan dokumentasi atas implikasi keamanan dari semua perubahan dalam koneksi jaringan eksternal atau pihak ketiga; 3) Pengaturan akses karyawan pihak ketiga ke data Bank yang sensitif atau kritikal dalam sistem yang di-*hosting* Bank dan pihak ketiga dilacak secara aktif berdasarkan prinsip hak istimewa; 4) Otentikasi yang kuat untuk mengamankan semua akses pihak ketiga ke jaringan dan/atau sistem dan aplikasi institusi; 5) Pemantauan dan pengujian kontrol untuk primer dan cadangan koneksi eksternal atau pihak ketiga secara berkala; 6) Kontrol keamanan yang dirancang dan diverifikasi untuk mendeteksi dan mencegah intrusi dari koneksi eksternal atau pihak ketiga; 7) Kejelasan tanggung jawab untuk menanggapi insiden keamanan siber serta pemberitahuan atas insiden dan kerentanan keamanan siber oleh 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 yang terhubung ke jaringan Bank; dan

				9) Terdapat proses pembaharuan diagram aliran data jaringan serta sistem dari koneksi eksternal dan pihak ketiga yang terhubung ke jaringan Bank dalam hal terjadi perubahan dan ditinjau secara periodik.
			Bank menerapkan manajemen risiko terkait keamanan siber untuk pihak ketiga.	
			Bank menetapkan standar minimum kendali keamanan siber bagi pihak ketiga, yaitu: a. Ketentuan kerahasiaan di kontrak kerja; b. Ketersediaan tata kelola pengamanan siber di pihak ketiga (kebijakan, prosedur, ketentuan, dan lainnya); dan c. Pengelolaan risiko terkait keamanan siber termasuk manajemen insiden siber di pihak ketiga.	
			Bank memiliki limit risiko terkait keamanan siber yang sesuai dengan tingkat risiko yang akan diambil, toleransi Risiko, dan strategi Bank terkait keamanan siber secara keseluruhan serta dengan memperhatikan kemampuan Bank untuk dapat menyerap eksposur risiko atau kerugian yang timbul, pengalaman kerugian di masa lalu, kemampuan sumber daya manusia, dan kepatuhan terhadap ketentuan eksternal yang berlaku.	Dalam rangka pengendalian risiko terkait keamanan siber, limit digunakan sebagai ambang batas untuk menentukan tingkat intensitas mitigasi risiko terkait keamanan siber yang akan dilaksanakan manajemen.
			Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber harus didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.	
			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 dan Sistem Informasi Manajemen Risiko Terkait Keamanan Siber	Identifikasi Risiko	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 pihak internal (sumber daya manusia, proses, dan sistem) maupun faktor eksternal Bank, dengan penjelasan sebagai berikut: 1) Sumber Daya Manusia (SDM) SDM merupakan sumber dari risiko terkait keamanan siber dalam bentuk ketidakmampuan SDM dalam melaksanakan tugas terkait pengamanan aset dan informasi 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 keamanan siber bagi Bank. Kelemahan dalam proses tersebut antara lain dapat mencakup tidak adanya proses *secure channel* saat transmisi, audit aspek keamanan tidak dilaksanakan secara berkala, manajemen *password* yang buruk, penggunaan akses internet publik yang tidak aman. 3) Sistem Kelemahan pada TI dan infrastruktur Bank dapat menjadi sumber risiko 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 Eksternal Faktor eksternal yang menjadi penyebab utama risiko siber bagi Bank adalah kurangnya *security awareness* dari nasabah. Selain itu, semakin berkembangnya taktik dan kecanggihan pelaku serangan siber juga menjadi faktor eksternal yang mengakibatkan munculnya risiko siber.
			Bank memastikan tersedianya metode atau sistem untuk melakukan identifikasi risiko pada seluruh kegiatan Bank yang terkait dengan keamanan siber.	
		Pengukuran Risiko	Bank melakukan pengukuran risiko secara berkala untuk seluruh kegiatan Bank yang terkait dengan keamanan siber.	

			Bank memiliki sistem pengukuran risiko untuk mengukur eksposur risiko terkait keamanan siber pada Bank sebagai acuan untuk melakukan pengendalian.	Sistem tersebut paling sedikit harus dapat mengukur: 1) sensitivitas kegiatan Bank yang terkait dengan keamanan siber terhadap perubahan faktor yang mempengaruhinya, 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 yang terkait dengan keamanan siber. Metode pengukuran risiko dapat dilakukan secara kuantitatif dan/atau kualitatif. Pemilihan metode pengukuran disesuaikan dengan karakteristik dan kompleksitas kegiatan usaha Bank.
			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.	
		Pemantauan Risiko	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, kepatuhan limit internal, dan hasil *stress testing* maupun konsistensi pelaksanaan dengan kebijakan dan prosedur yang ditetapkan.	Pemantauan dilakukan baik oleh unit pelaksana 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 tindakan yang diperlukan.
			Bank menyiapkan suatu sistem *back-up* dan prosedur 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.	

		Pengendalian Risiko	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 dan toleransi risiko. Pengendalian risiko terkait keamanan siber dapat dilakukan oleh Bank terkait keamanan siber, antara lain penyediaan sistem *back-up* dan penyelenggaraan rencana pemulihan bencana (*disaster recovery plan*/DRP).
		Sistem Informasi Manajemen Risiko terkait Keamanan Siber	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 harus dapat memastikan: 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 memigitas 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; dan 3) tersedianya informasi tentang hasil atau realisasi penerapan manajemen risiko terkait keamanan siber dibandingkan yang ditetapkan oleh Bank sesuai dengan kebijakan dan strategi penerapan manajemen risiko terkait keamanan siber.
			Bank memastikan sistem informasi manajemen risiko terkait keamanan siber dan informasi yang dihasilkan sesuai dengan karakteristik dan kompleksitas kegiatan usaha Bank serta adaptif terhadap perubahan.	
			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.	

			Sebagai bagian dari sistem informasi manajemen risiko terkait keamanan siber, laporan maturitas keamanan siber disusun secara berkala oleh unit dan fungsi yang bertugas menangani ketahanan dan keamanan siber Bank. Frekuensi penyampaian laporan kepada Direksi terkait dan komite manajemen risiko harus ditingkatkan sesuai kebutuhan terutama dalam hal kondisi pasar berubah dengan cepat.	
			Bank memastikan sistem informasi manajemen risiko terkait keamanan siber harus mendukung pelaksanaan pelaporan kepada Otoritas Jasa Keuangan.	
4	Sistem Pengendalian Intern		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 yang dimaksud menjadi tanggung jawab seluruh satuan kerja bisnis dan satuan kerja pendukung termasuk satuan kerja kepatuhan, satuan kerja manajemen risiko, dan satuan kerja audit internal. Dalam menerapkan sistem pengendalian internal dimaksud, Bank secara umum memperhatikan antara lain: a) penerapan manajemen risiko terkait keamanan siber telah mencapai hasil yang diharapkan; b) kesesuaian antara sistem pengendalian intern dengan tingkat risiko inheren dan penerapan manajemen risiko terkait keamanan siber pada Bank; c) penetapan wewenang dan tanggung jawab untuk pemantauan kepatuhan kebijakan dan prosedur manajemen risiko terkait keamanan siber serta penetapan limit risiko terkait keamanan siber; d) 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; e) struktur organisasi yang menggambarkan secara jelas tugas dan tanggung jawab masing-masing unit dan individu;

			f) pelaporan penerapan manajemen risiko terkait keamanan siber termasuk insiden dan respon atas ancaman keamanan siber yang akurat dan tepat waktu; g) kecukupan prosedur untuk memastikan kepatuhan Bank terhadap ketentuan dan peraturan perundang-undangan; h) kaji ulang yang efektif, independen, dan obyektif terhadap kebijakan, kerangka dan prosedur manajemen risiko terkait keamanan siber Bank; i) pengujian dan kaji ulang yang memadai terhadap sistem informasi manajemen risiko terkait keamanan siber; j) dokumentasi secara lengkap dan memadai terhadap cakupan, prosedur operasional, temuan audit, tanggapan berdasarkan hasil audit terhadap keamanan siber, serta tindak lanjut hasil audit; dan k) verifikasi dan kaji ulang secara berkala dan berkesinambungan terhadap penanganan kelemahan Bank yang bersifat material dan tindakan untuk memperbaiki penyimpangan yang terjadi terhadap keamanan siber.
		Bank melaksanakan sistem pengendalian intern secara efektif dalam penerapan proses ketahanan siber dengan mengacu pada kebijakan dan prosedur yang telah ditetapkan.	a) semua tanggung jawab keamanan siber dan keamanan informasi telah ditentukan dan dialokasikan serta terkoordinasi dengan baik; b) kepatuhan atas kewajiban semua sumber daya manusia termasuk kontraktor untuk menerapkan keamanan siber sesuai dengan kebijakan dan prosedur yang telah ditetapkan; c) kecukupan persyaratan keamanan siber terkait akses *supplier* terhadap aset TI Bank yang telah didokumentasikan dengan baik; d) kecukupan pengujian terhadap keberadaan informasi yang dapat berguna bagi penyerang seperti *network diagram*, *file* konfigurasi, laporan *penetration testing*, *email*, atau dokumen yang berisikan kata sandi atau informasi lain yang penting untuk sistem operasi; e) kecukupan penetapan program untuk *vulnerability assessment* atau *penetration testing* secara berkala kepada aplikasi web, aplikasi *client-based*, aplikasi *mobile*, *wireless*, server, dan perangkat jaringan; f) kecukupan kualitas dan kuantitas SDM, cakupan tugas serta tanggung jawab *red-team* (*offensive security professionals* yang melakukan penyerang atas sistem) dan *blue-team* (*defensive security professionals* yang melakukan pertahanan atas sistem) serta pengujian secara berkala yang dilakukan dalam mengukur kesiapan Bank untuk mengidentifikasi dan menghentikan serangan atau merespons dengan cepat dan efektif dari insiden keamanan yang terjadi;

			g) pemisahan lingkungan (*environment*) antara sistem produksi dengan pengembangan serta prosedur izin akses kepada pengembangan tanpa adanya pengawasan dari bagian keamanan siber Bank; h) 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; i) perlindungan aplikasi web Bank dengan menggunakan *firewall* aplikasi web (WAFs) serta memastikan bahwa perlindungan tersebut berjalan disemua perangkat komputasi; j) perlindungan alamat IP internal Bank dengan menggunakan NAT (*Network Address Translation*); k) penggunaan *intrusion detection system* (IDS) dan *intrusion prevention system* (IPS); l) penggunaan anti virus dan anti *malware* yang dilakukan secara terpusat dan selalu dikinikan terhadap perangkat *endpoint*; m) penggunaan *data loss prevention* (DLP) atau *network access control* (NAC); n) pelaksanaan *risk assessment* terhadap risiko terkait keamanan siber secara berkala; o) pencegahan atau pengurangan terhadap dampak/efek yang tidak diinginkan dari risiko terkait keamanan siber maupun peluang yang dimiliki oleh Bank; p) penerapan pengendalian keamanan (*security control*) untuk meminimalisir risiko; q) ketersediaan dan kecukupan *risk register* terkait keamanan siber yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria Bank, antara lain atas seluruh aplikasi yang memproses *data stakeholder* Bank; r) penerapan *continual improvement* terhadap keamanan siber; s) implementasi kebijakan *domain-based massage authentication and conformance* (DMARC) atau protokol otentikasi *email* untuk melindungi domain dari pengunaan yang tidak sah agar tidak digunakan dalam serangan penyusupan *email* bisnis, *email phising*, penipuan *email*, *email* palsu, dan aktivitas ancaman keamanan siber lainnya; t) filterisasi terhadap seluruh jenis *file* lampiran *email*; u) penerapan metode *sandbox* terhadap seluruh lampiran *email* untuk mencegah dan analisis keamanan lebih lanjut terhadap *malicious behavior*; dan v) integrasi keamanan siber dalam seluruh fase perencanaan, pembangunan, dan pengembangan semua proyek TI.

		Bank harus 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 menangani fungsi manajemen risiko terkait keamanan siber dan satuan kerja audit internal.
		Bank memastikan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber melakukan kaji ulang dan evaluasi secara memadai.	Penerapan kaji ulang dan evaluasi secara umum mencakup antara lain: a. kesesuaian kerangka manajemen risiko terkait keamanan siber, yang mencakup kebijakan, struktur organisasi, alokasi sumber daya, desain proses manajemen risiko, sistem informasi, pelaporan risiko operasional Bank, dan pelaksanaan manajemen terkait risiko terkait keamanan siber; b. metode, asumsi, dan variabel yang digunakan untuk mengukur risiko terkait keamanan siber dan limit eksposur risiko terkait keamanan siber; c. perbandingan antara hasil dari metode pengukuran risiko terkait keamanan siber yang menggunakan simulasi atau proyeksi pada masa datang dengan hasil aktual; d. perbandingan antara asumsi yang digunakan dalam metode dimaksud dengan kondisi yang sebenarnya atau aktual; e. perbandingan antara limit risiko terkait keamanan siber yang ditetapkan dengan eksposur risiko terkait keamanan siber yang sebenarnya atau aktual; dan f. penerapan manajemen risiko terkait keamanan siber oleh satuan kerja bisnis atau satuan kerja pendukung.
		Bank memastikan satuan kerja internal audit melakukan kaji ulang dan evaluasi secara memadai.	Penerapan kaji ulang dan evaluasi secara umum mencakup antara lain: a. 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 risiko Bank; b. penerapan manajemen risiko terkait keamanan siber oleh seluruh pegawai, termasuk kaji ulang terhadap pelaksanaan pemantauan oleh satuan kerja yang berfungsi menangani manajemen risiko terkait keamanan siber; c. penerapan manajemen data termasuk pelindungan; d. pengunaan algoritma enkripsi dalam pengembangan perangkat lunak; e. penggunaan *tool vulnerability scanning* secara mandiri, yang mana hasil *vulnerability assessment* digunakan sebagai titik awal dalam melakukan *penetrating testing*; f. penggunaan akun khusus selain akun admin untuk melakukan *vulnerability testing*;

			g. pengendalian dan pemantauan atas akun pengguna atau sistem yang digunakan dalam melakukan *penetration testing* untuk memastikan bahwa akun tersebut hanya digunakan untuk tujuan yang sah dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan; h. penerapan keamanan informasi; i. pelaksanaan secara berkala *security risk assessment* dan *security risk treatment*; j. izin akses dari pengguna setidaknya setiap tiga bulan; k. dokumentasi/diagram yang menggambarkan semua aliran data di seluruh sistem dan jaringan termasuk pembaruannya; dan l. penerapan dan dokumentasi standar konfigurasi (*port, protocol, service*) untuk semua sistem, seperti *operating system*, *software* atau aplikasi.
		Bank memastikan pihak yang melakukan kaji ulang dan evaluasi manajemen risiko terkait keamanan siber harus independen dan memiliki kompetensi yang baik serta metode kaji ulang yang andal.	
		Hasil kaji ulang dan evaluasi tersebut disampaikan kepada Dewan Komisaris dan Direksi untuk diambil langkah perbaikan dan/atau penyempurnaan manajemen risiko terkait keamanan siber.	
		Satuan kerja internal audit melakukan pemantauan terhadap perbaikan hasil temuan. Temuan yang belum ditindaklanjuti harus dilaporkan kepada Dewan Komisaris dan/atau Direksi untuk diambil langkah-langkah yang diperlukan.	
		Bank memiliki sistem rotasi rutin untuk menghindari potensi *self-dealing*, persekongkolan atau penyembunyian suatu dokumentasi atau aktivitas yang tidak wajar.	

I.c Penilaian Kualitas Penerapan Proses Ketahanan Siber

Matriks Parameter atau Indikator Penilaian Kualitas Penerapan Proses Ketahanan Siber

No.	Domain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
1	Proses Identifikasi Aset, Ancaman, dan Kerentanan	Bank menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, sumber daya manusia, jaringan, dan infrastruktur) dan pencatatan konfigurasi secara efektif.	Dalam melakukan manajemen aset TI, Bank: 1) melakukan inventarisasi aset TI antara lain perangkat keras, perangkat lunak, data, sumber daya, jaringan, dan infrastruktur untuk menetapkan prioritisasi 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*. 4) melakukan inventarisasi aset TI secara berkala.
		Bank melakukan *vulnerability assessment* dan pemantauan terhadap perkembangan siber terkini untuk mengidentifikasi ancaman siber.	1) melakukan pemantauan seluruh sistem secara berkala untuk mengidentifikasi kelemahan dan kerentanan (*vulnerability assessment*). Frekuensi pelaksanaan *vulnerability assessment* 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 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 dapat ditimbulkan; dan 4) menyusun dan memelihara inventaris risiko (*risk register*).
		Bank melakukan pengujian keamanan siber secara berkala.	1) melakukan pengujian keamanan siber berdasarkan analisis kerentananan. 2) melakukan pengujian keamanan siber berdasarkan skenario. 3) melakukan upaya secara proaktif untuk menyusun skenario pengujian yang realistis, antara lain melalui *threat hunting* yang menyeluruh.

2	Proses Pelindungan Aset	Bank menerapkan pengendalian keamanan (*security control*) yang komprehensif.	Pengendalian keamanan yang komprehensif diterapkan sesuai dengan hasil identifikasi atas aset, ancaman, dan kerentanan yang telah dilakukan sebelumnya, dengan bertujuan untuk memastikan: 1) keberlangsungan dan ketersediaan sistem informasi; 2) integritas, kerahasiaan, serta ketersediaan data dan informasi; dan 3) kesesuaian dengan ketentuan peraturan perundang-undangan dan standar yang berlaku.
		Bank melakukan pemeliharaan dan perbaikan terhadap pengendalian keamanan atas aset TI sesuai dengan kebijakan dan prosedur yang berlaku.	
		Bank menerapkan sistem pengamanan yang dikelola dengan baik sesuai dengan kebijakan dan prosedur yang berlaku.	Memiliki kebijakan dan prosedur terkait dengan penerapan sistem pengamanan serta memastikan kebijakan dan prosedur tersebut diterapkan dengan baik.
		Bank memperbarui pengendalian keamanannya secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan sesuai dengan proses identifikasi terkini.	Meninjau pengendalian keamanan siber yang diterapkan pada Bank sesuai dengan kritikalitas aset TI berdasarkan identifikasi terkini.
		Bank menerapkan manajemen keamanan data dan informasi dan memastikan bahwa data dan/atau informasi dikelola sesuai dengan strategi risiko organisasi untuk melindungi kerahasiaan, integritas, dan ketersediaan data serta informasi.	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) Mekanisme pengecekan integritas untuk melakukan verifikasi atas integritas perangkat lunak, *firmware*, perangkat keras serta data dan informasi; 4) Pelindungan terhadap ketersediaan data dan informasi, dengan memperhatikan kepemilikan, periode retensi, dan penggunaan data dan informasi; 5) Pemisahan antara lingkungan pengembangan dan pengujian (*development and testing environment*) dari lingkungan produksi (*production environment*); 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) Dalam hal terdapat kebutuhan untuk menerima atau menyampaikan data dan/atau informasi dari atau kepada pihak ketiga, Bank melakukan

			pengamanan, dokumentasi, serta pemantauan atas penggunaan data dan/atau informasi dimaksud; dan 8) Penerapan metode otomatis untuk sinkronisasi waktu atas *critical system clocks* dengan menggunakan protokol seperti *Network Time Protocol*.
		Bank menerapkan manajemen pelindungan terhadap jaringan, perangkat keras, dan perangkat lunak.	1) memiliki perangkat pelindungan jaringan perimeter (misalnya *border router* dan *firewall*) yang memadai dan diverifikasi secara berkala, termasuk *implicit* atau *explicit deny rule*; 2) memiliki *Intrusion Prevention System* (IPS) untuk menghalangi percobaan serangan atau gangguan; 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 diaplikasikan; 5) melakukan pemantauan terhadap *port* jaringan secara berkala; 6) menggunakan autentifikasi terpusat untuk seluruh perangkat jaringan; 7) memastikan dilakukannya proses enkripsi untuk autentifikasi dan transmisi data melalui jaringan nirkabel dan perangkat *mobile* baik milik Bank maupun pengguna, serta media penyimpanan eksternal; 8) memiliki perangkat keamanan jaringan, misalnya *Domain Name System* (DNS) *filtering service* atau DNS *Security Extensions*; 9) memiliki sistem pengecekan otomatis terhadap *spam/phising/malware* pada *email* termasuk yang ada di dalam *cloud*; 10) menggunakan pembatasan penggunaan *scripting tools* (misalnya *Microsoft PowerShell* dan *Phyton*); 11) memastikan seluruh jaringan, aplikasi, dan perangkat TI Bank masih mendapatkan *update support*, antara lain mencakup web *browser*, *email client*, sistem operasi, *database server*, perangkat jaringan, perangkat *security*, serta memastikan *update support* tersebut segera dilakukan dalam hal terdapat *security patches*; 12) menggunakan *add-on* dan *plugin* aplikasi sesuai dengan ketentuan organisasi; 13) memastikan: a) kecukupan proses formal pengelolaan konfigurasi *router*, *switch* dan *firewall*, meliputi perubahan dan pengujian semua 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 configs* dengan *running configs*; d) kebijakan akun *default* konfigurasi, serta *back-up* atas konfirugasi perangkat tersebut; 14) mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan; 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 (seperti: *port* USB, DVD, akses *smartphone*, dan lainnya); dan 18) menerapkan *whitelist* aplikasi untuk memastikan bahwa hanya *authorized software library* dan *signed script* yang dapat dijalankan oleh sistem.
		Bank menerapkan manajemen pelindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastuktur jaringan, dan komponen sistem yang dikelola oleh Bank.	1) mengimplementasikan identifikasi dan autentifikasi pengelolaan akses terhadap seluruh sistem, aplikasi, dan *hardware*; 2) melakukan kendali terhadap akses pengguna, termasuk *password complexity*, pembatasan percobaan dan penggunaan kembali *password* serta permintaan *password* setelah perangkat tidak aktif untuk beberapa saat; 3) menerapkan pengamanan *endpoint* antara lain dengan menggunakan web URL *filtering*, *device control*, dan aplikasi *control* pada seluruh perangkat *end-point* pengguna termasuk *end-point* yang terhubung ke 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; 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 *work station* untuk mencegah terjadinya serangan siber dan *disabled peer to peer* pada *wireless client* di perangkat; 9) memastikan /pegawai *end-point* 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 autentifikasi melalui saluran terenkrepsi, baik untuk login terhadap jaringan maupun aplikasi.

		Bank menerapkan pelindungan yang memadai dalam penggunaan *cloud computing* sesuai dengan *service cloud* yang digunakan, dalam hal Bank menggunakan *cloud computing*.	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 (*security in the cloud*) telah dikonfigurasikan sesuai standar dan *best practices*; 4) memastikan kapabilitas SDM Bank untuk dapat mengonfigurasi 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 *Multi-Factor Authentication* (MFAs); 9) memastikan penyedia *cloud* memiliki *Data Center Redundancy* yang terpisah secara geografis dan memiliki *Recovery Point* dan *Recovery Time Objective* yang terdokumentasi; dan 10) memastikan penerapan *single-sign on* serta aksesnya melalui SSL VPN *tunnel*.
		Bank memastikan penerapan *secure coding* dalam pengembangan sistem dan aplikasi untuk memastikan integritas sistem dan aplikasi.	1) memastikan *developer* 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 *integrated development environment* yang digunakan; dan 4) melakukan *review* dan pengujian secara berkala terhadap keamanan *software* yang dikembangkan oleh internal Bank maupun pihak ketiga.
		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.	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 prioritisasi 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	Bank memastikan ketersediaan dokumentasi kinerja dasar (*baseline performance*) atas fungsi kritis Bank dan sistem pendukung, sehingga setiap penyimpangan dapat dideteksi secara tepat waktu dan aktivitas serta kejadian anomali dapat ditandai untuk diselidiki.	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 siber dan tetap sepadan dengan ancaman dan kerentanan siber Bank; dan 5) melakukan sentralisasi dan mengoordinasi proses keamanan siber dan teknologi (Contoh: *Security Operations Center* (SOC) atau yang sejenis).
		Bank melakukan pemantauan atau deteksi secara berkelanjutan terhadap kerentanan untuk memastikan efektivitas upaya pelindungan yang telah diterapkan.	1) melakukan deteksi terhadap *malicious code*, deteksi terhadap *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 efektifitas tindakan pelindungan yang dilakukan; 3) melakukan upaya untuk mendeteksi adanya *malicious domain.* (Contoh: dengan DNS *query logging* untuk mengetahui adanya *unauthorized domain*); 4) melakukan *review* 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; dan 6) melakukan upaya untuk memperoleh informasi terkini mengenai keamanan siber (Contoh: melalui *managed security service provider* atau penyedia produk keamanan siber, *multiple threat intelligence feeds*, dan *cyber threat intelligence unit*).
		Bank melakukan pemantauan atas aktivitas mencurigakan serta melakukan pengelolaan dan pengujian proses maupun prosedur deteksi untuk memastikan aktivitas anomali dapat dideteksi secara tepat waktu.	1) mengimplementasikan *Enable 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* pada *log server* yang tersentralisasi untuk mencegah akses atau perubahan audit *log* yang tidak diautorisasi dan memastikan kapasitas penyimpanan *log* sesuai dengan kebutuhan; 4) melakukan deteksi atas akses yang tidak diautorisasi, kegagalan *login* pada perangkat jaringan, server, dan aplikasi, serta anomali pada jaringan; 5) memiliki sistem peringatan atas aktivitas mencurigakan serta ditindaklanjuti dan dikomunikasikan kepada pihak/stakeholder terkait; dan 6) melakukan prioritisasi atas kejadian (*event*) dalam *log* berdasarkan tingkat keparahan/dampak, dan kategori keamanan.
		Bank memastikan ketersediaan proses untuk mendeteksi insiden secara memadai.	1) memastikan mekanisme deteksi (antivirus and *antimalware alerts*, *log event alerts*, perangkat pengamanan) berjalan dengan baik untuk memberikan peringatan atas insiden atau serangan; 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 kejadian dan insiden yang terjadi; dan 5) memastikan adanya proses pencatatan terhadap insiden yang terdeteksi sesuai dengan kategorisasi kejadian berdasarkan *severity level*/prioritas/dampak, kategori keamanan, dan jenis *log* yang berkorelasi (Contoh: dengan menggunakan *ticketing system*).
		Bank 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.	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 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	Bank memiliki rencana penanggulangan dan pemulihan saat insiden siber terjadi untuk memastikan penanggulangan yang tepat waktu dalam mengembalikan layanan secepat mungkin dengan dampak minimal.	1) kategorisasi fungsi kritis sebagaimana proses identifikasi untuk menentukan prioritas pemulihan sistem dan layanan; 2) memiliki rencana *re-route* atau penggantian fungsi kritikal yang terdampak insiden siber; 3) pelaporan dan eskalasi di intern Bank, termasuk kepada *senior management*, 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; 5) menguraikan alur komunikasi kepada pemangku kepentingan internal dan eksternal yang perlu dikomunikasikan tentang insiden siber dan praktik/teknik serangan siber yang berkembang saat ini yang berpotensi meningkatkan risiko terjadinya *fraud*, termasuk waktu pemberitahuan, dan cakupan informasi yang perlu dikomunikasikan. Tingkat keterlibatan pemangku kepentingan ditentukan oleh *severity level* dan dampak insiden siber; 6) Bank mempertimbangkan berbagai skenario insiden siber dalam merumuskan rencana penanggulangan dan pemulihan serta melakukan analisis dampak atas insiden terhadap aktivitas Bank; dan 7) Rencana penanggulangan dan pemulihan harus sesuai dengan *business continuity plan*, *disaster recovery plan*, *crisis management plan*, dan/atau kebijakan atau rencana Bank lainnya yang terkait.
		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.	
		Bank menerapkan prosedur pemulihan dan upaya untuk mencegah suatu insiden menjadi berkembang dengan memitigasi efek dan menanggulangi insiden tersebut.	1) memastikan pemahaman terhadap dampak dari insiden siber, pelaksanaan penyelidikan forensik, dan kategorisasi insiden siber; 2) Bank telah melakukan langkah penanggulangan dan pemulihan insiden siber sesuai dengan rencana;

			3) *root cause analysis* terhadap insiden siber untuk mencegah terulangnya kejadian serupa; 4) kaji ulang terhadap rekap laporan insiden siber untuk mempelajari kesesuaian prosedur insiden siber dengan standar dan prosedur yang telah ditetapkan; dan 5) mencatat setiap langkah yang dilakukan dalam rangka penanggulangan insiden sebagai pembelajaran (*lesson learned*) dari insiden siber yang terjadi untuk meningkatkan kapabilitas mitigasi risiko serta pembaharuan terhadap rencana penanganan dan pemulihan insiden siber Bank apabila diperlukan.
		Bank melakukan analisis untuk memastikan langkah penanggulangan dan pemulihan insiden siber dijalankan dengan tepat.	1) menerapkan isolasi insiden sebagai langkah mitigasi awal; 2) mengimplementasikan rencana *re-route* atau penggantian fungsi kritikal yang terdampak insiden siber; 3) melakukan upaya untuk mengembalikan operasional dengan gangguan layanan yang minimal sesuai dengan jenis insiden yang terjadi; dan 4) memiliki proses untuk memastikan aset TI yang terdampak oleh insiden siber dan tidak dapat digunakan kembali untuk kegiatan operasional telah digantikan, sehingga fungsi operasional tetap berjalan.
		Bank menerapkan eskalasi dan pelaporan atas insiden siber.	1) proses eskalasi kepada pihak yang berwenang untuk melakukan penanggulangan dan analisis insiden siber sesuai dengan *service level agreement* tertentu; 2) proses eskalasi untuk melaporkan pelaksanaan penanggulangan dan pemulihan insiden siber kepada *senior management*, Direksi, dan Dewan Komisaris berdasarkan kriteria potensi dampak dan kritikalitas; 3) prosedur 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; dan 4) memiliki *ticketing system* yang digunakan untuk melacak perkembangan terkini/*progress* dari penanggulangan dan pemulihan telah selesai (*event post-notification*) serta mengategorisasikan kejadian berdasarkan tingkat keparahan/prioritas/dampak, kategori keamanan, dan jenis *log* yang berkorelasi.

LAMPIRAN II

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR …

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

Teknologi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
1	Interkoneksi ke internet publik	Kurang atau sama dengan 2 koneksi	4 koneksi	6 koneksi	8 koneksi	Lebih atau sama dengan 10 koneksi		
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*		
3	Akses ke aset teknologi informasi (TI) internal Bank	Koneksi kabel hanya untuk pegawai	Koneksi kabel untuk pegawai saja dan Wi-Fi untuk pihak ketiga terotoriasasi	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		
4	Jaringan Intranet dari kantor cabang	Bank memiliki kantor cabang yang tersebar kurang dari 100 lokasi	Bank memiliki kantor cabang yang tersebar di lebih dari 100 hingga 300 lokasi	Bank memiliki kantor cabang yang tersebar di lebih dari 300 hingga 500 lokasi	Bank memiliki kantor cabang yang tersebar di lebih dari 500 hingga 700 lokasi	Bank memiliki kantor cabang yang tersebar di lebih dari 700 lokasi		
5	Penggunaan jasa *cloud service provider*	Tidak ada penggunaan jasa *cloud service provider*	Penggunaan jasa *cloud service provider* untuk *collaboration tools*	Penggunaan jasa *cloud service provider* untuk *collaboration tools* dan *platform* TI	Penggunaan jasa *cloud service provider* untuk *collaboration tools, platform* TI, dan infrastruktur TI	Terdapat data transaksional dan data pribadi nasabah yang disimpan/diproses dalam layanan yang menggunakan jasa *cloud service provider*		
6	Pengelolaan perangkat lunak yang digunakan untuk	Seluruh sistem/aplikasi yang	Lebih dari 70% sistem/aplikasi	Lebih dari 50% sistem/aplikasi	Lebih dari 30% sistem/aplikasi	Hingga 30% sistem/aplikasi yang		

	mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* dan TI).	digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI) dikelola (dikembangkan dan diselenggarakan) oleh tim TI Bank	yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI) dikelola (dikembangkan dan diselenggarakan) oleh tim TI Bank	yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI) dikelola (dikembangkan dan diselenggarakan) oleh tim TI Bank	yang digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* & TI) dikelola (dikembangkan dan diselenggarakan) oleh tim TI Bank	digunakan untuk mendukung kegiatan operasional Bank (termasuk kebutuhan *back-office* dan TI) dikelola (dikembangkan dan diselenggarakan) oleh tim TI Bank		
7	Penggunaan perangkat keras dan/atau perangkat lunak yang sudah dan/atau akan memasuki masa *End-of-life* (EOL)	Tidak ada sistem (perangkat keras ataupun perangkat lunak) yang melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Hingga 30% sistem (perangkat keras ataupun perangkat lunak) yang melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Hingga 50% sistem (perangkat keras ataupun perangkat lunak) yang melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Hingga 70% sistem (perangkat keras ataupun perangkat lunak) yang melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)	Lebih dari 70% sistem (perangkat keras ataupun perangkat lunak) yang melebihi masa EOL atau mendekati masa EOL (2 tahun ke depan akan memasuki masa EOL)		
8	Jumlah Pegawai yang dapat memiliki akses koneksi perangkat pribadi ke jaringan Bank (kebijakan *Bring Your Own Device*/BYOD)	Tidak diperbolehkan penggunaan perangkat pribadi (BYOD)	BYOD diperbolehkan untuk 1 jenis perangkat kepada kurang dari 5% pegawai tertentu	BYOD diperbolehkan untuk 1 jenis perangkat kepada kurang dari 10% pegawai tertentu	BYOD diperbolehkan untuk 1 jenis perangkat kepada kurang dari 25% pegawai tertentu	BYOD diperbolehkan untuk seluruh jenis perangkat kepada 25% pegawai tertentu		
9	Perangkat lunak yang dapat diakses menggunakan perangkat pribadi ke jaringan Bank (kebijakan *Bring Your Own Device*/BYOD)	Tidak diperbolehkan penggunaan perangkat pribadi (BYOD)	Perangkat pribadi yang terhubung ke jaringan kantor hanya dapat mengakses *email*	Perangkat pribadi yang terhubung ke jaringan kantor hanya dapat mengakses *email* dan aplikasi	Perangkat pribadi yang terhubung ke jaringan kantor dapat mengakses aplikasi kritikal	Perangkat pribadi yang terhubung ke jaringan kantor dapat mengakses seluruh sistem/aplikasi (termasuk *core banking system*)		

				penunjang (tidak bersifat kritikal)				
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 jaringan internal Bank	Jumlah Minimal (1 – 3 perusahaan atau kurang dari 10 individu)	Jumlah Moderate (4 – 6 perusahaan atau kurang dari 20 individu)	Jumlah Signifikan (7 – 10 perusahaan atau kurang dari 30 individu)	Jumlah Substansial (Lebih dari 10 perusahaan atau lebih dari 30 individu)		

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

Produk Bank		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
1	Penggunaan Saluran *Online* dan *Mobile* dalam memberikan layanan	Tidak ada aplikasi (baik *back-office* maupun untuk nasabah) yang menggunakan saluran *online* dan *mobile*	Saluran *online* dan *mobile* digunakan untuk penyampaian informasi umum Bank kepada masyarakat (antara lain notifikasi/berita, lokasi kantor cabang, produk Bank yang tersedia)	Saluran *online* dan *mobile* digunakan untuk pelayanan transaksi perbankan (produk Bank) bagi nasabah *wholesale* secara domestik	Saluran *online* dan *mobile* digunakan untuk pelayanan transaksi perbankan (produk Bank) bagi nasabah *retail* secara domestik	Saluran *online* dan *mobile* digunakan untuk: 1. kebutuhan produk nasabah *wholesale* dan *retail* termasuk remitansi luar negeri dan pertukaran mata uang; dan/atau 2. interkoneksi dengan ekosistem ekonomi digital (*Super App*)		
2	Mekanisme pengelolaan *automated teller machine* (ATM)	Bank tidak memiliki layanan ATM	Layanan ATM tersedia, namun bank tidak memiliki mesin ATM	Layanan ATM tersedia, mesin ATM dan proses pengisian uang dikelola oleh pihak ketiga	Layanan ATM tersedia, mesin ATM dan proses pengisian uang dikelola dengan kombinasi antara internal Bank dan pihak ketiga	Layanan ATM tersedia, mesin ATM dan pengisian uang dikelola sepenuhnya oleh internal Bank		
3	Produk Bank berupa alat pembayaran menggunakan kartu (kartu debit, kartu kredit, dan/atau *prepaid card*)	Bank tidak menerbitkan alat pembayaran menggunakan kartu	Bank hanya menerbitkan kartu debit	Bank menerbitkan alat pembayaran menggunakan kartu	Bank menerbitkan alat pembayaran menggunakan kartu untuk Bank lain/institusi keuangan lain (1-5)	Bank menerbitkan alat pembayaran menggunakan kartu untuk Bank lain/institusi keuangan lain (>5)		
4	Jenis Produk Bank Berbasis Teknologi Informasi	Bank tidak memiliki produk berbasis TI	Bank memiliki produk berbasis TI	Bank memiliki produk berbasis TI untuk *funding,*	Bank memiliki produk berbasis TI untuk *funding,*	Bank memiliki produk berbasis TI untuk *funding, lending,*		

			untuk *funding* dan/atau *lending*	*lending*, dan/atau *treasury*	*lending, treasury,* dan/atau aktivitas sistem pembayaran dan investasi pasar modal untuk kebutuhan domestik	*treasury,* dan/atau aktivitas sistem pembayaran termasuk jual beli mata uang dan investasi pasar modal untuk kebutuhan internasional		
5	Bank sebagai penyedia jasa TI	Bank tidak menjadi penyedia jasa TI untuk entitas lain	Bank menjadi penyedia jasa TI untuk < 3 entitas lain	Bank menjadi penyedia jasa TI untuk hingga 3 entitas lain	Bank menjadi penyedia jasa TI untuk hingga 5 entitas lain	Bank menjadi penyedia jasa TI untuk lebih dari 5 entitas 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

Karakteristik Organisasi		Level Risiko					Hasil Penilaian[1)]	Penjelasan[2)]
		***Low* (1)**	***Low to Moderate* (2)**	***Moderate* (3)**	***Moderate to High* (4)**	***High* (5)**		
1	Organisasi Keamanan Siber	Peran dan tanggung jawab keamanan siber telah terintegrasi secara menyeluruh di organisasi	Peran dan tanggung jawab keamanan siber telah terintegrasi secara menyeluruh dengan layanan TI yang tersedia, manajemen risiko, dan audit internal	Peran dan tanggung jawab keamanan siber telah terintegrasi secara menyeluruh dengan layanan TI yang tersedia	Peran dan tanggung jawab keamanan siber belum terintegrasi secara menyeluruh dengan layanan TI yang tersedia	Tidak terdapat peran dan tanggung jawab terkait keamanan siber yang di Bank		
2	Posisi/Jabatan Keamanan Siber	Seluruh posisi manajerial terkait pengamanan siber terisi dalam 3 tahun terakhir	Seluruh posisi manajerial terkait pengamanan siber terisi dalam 2 tahun terakhir	Seluruh posisi manajerial terkait pengamanan siber terisi dalam 1 tahun terakhir	Terdapat posisi manajerial terkait pengamanan siber yang kosong	Tugas dan tanggung jawab dari posisi manajerial terkait pengamanan siber belum didefinisikan		
3	Perubahan (*Turnover*) pada SDM di TI/Keamanan Siber	Tidak ada pergantian dari personil di TI/Keamanan Siber dalam 1 tahun terakhir.	Persentase pergantian personil di TI/Keamanan Siber <5% dalam 1 tahun terakhir.	Persentase pergantian personil di TI/Keamanan Siber <10% dalam 1 tahun terakhir.	Persentase pergantian personil di TI/Keamanan Siber <15% dalam 1 tahun terakhir.	Persentase pergantian personil di TI/Keamanan Siber ≥ 15% dalam 1 tahun terakhir.		
4	Perubahan di lingkungan TI	1-2 implementasi sistem dengan risiko tinggi dalam 1 tahun terakhir.	3-5 implementasi sistem dengan risiko tinggi dalam 1 tahun terakhir.	6-8 implementasi sistem dengan risiko tinggi dalam 1 tahun terakhir.	9-11 implementasi sistem dengan risiko tinggi dalam 1 tahun terakhir.	>11 implementasi sistem dengan risiko tinggi dalam 1 tahun terakhir.		
5	Pengelolaan *privilege access* (administrator dan selevel administrator) di seluruh perangkat (*host*, jaringan, *database*, aplikasi, dan *cloud*).	Seluruh *privilege access* untuk seluruh perangkat dikelola oleh unit TI	*Privilege access* untuk sekitar 2 tipe perangkat dikelola oleh pihak selain unit TI	*Privilege access* untuk sekitar 3 tipe perangkat dikelola oleh pihak selain unit TI	*Privelege access* untuk sekitar 4 tipe perangkat dikelola oleh pihak selain unit TI	*Privelege access* untuk sekitar 5 tipe perangkat dikelola oleh 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

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)**		
1	Jumlah Insiden Siber dalam 12 bulan terakhir	Tidak ada insiden siber yang dilaporkan	Hingga 30% dari total insiden siber yang dilaporkan berdampak signifikan	Hingga 50% dari total insiden siber yang dilaporkan berdampak signifikan	Hingga 70% dari total insiden siber yang dilaporkan berdampak signifikan	Lebih dari 70% dari total insiden siber yang dilaporkan berdampak signifikan		

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	Pengawasan Aktif Direksi dan Komisaris	Bank menetapkan wewenang dan tanggung jawab Dewan Komisaris terkait dengan penerapan manajemen risiko terkait keamanan siber.				
...	...	...	...				
...	...	...	...				

Keterangan:

1) Diisi dengan domain, subdomain, dan kontrol sebagaimana pada Lampiran I.b. Matriks Parameter atau Indikator Penilaian Kualitas 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 dapat mempertimbangkan penjelasan/kriteria pemenuhan kontrol sebagaimana pada Lampiran I.b. Matriks Parameter atau Indikator Penilaian Kualitas 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	Bank menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, sumber daya manusia, jaringan, dan infrastruktur) dan pencatatan konfigurasi secara efektif.				
...	...	...				
...	...	...				

Keterangan:

1) Diisi dengan domain dan kontrol sebagaimana pada Lampiran I.c. Matriks Parameter atau Indikator Penilaian Kualitas 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 dapat mempertimbangkan penjelasan/kriteria pemenuhan kontrol sebagaimana pada Lampiran I.c. Matriks Parameter atau Indikator Penilaian Kualitas 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.

LAMPIRAN III

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR ...

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 datang. Contoh karakteristik bank yang termasuk dalam peringkat *Low* (1) antara lain sebagai berikut: a. Bank menggunakan teknologi informasi yang sangat terbatas. Kerentanan terhadap gangguan atau serangan sangat rendah. b. Produk bank yang disalurkan menggunakan teknologi dan/atau jaringan *online* dan *mobile* sangat terbatas dengan volume transaksi yang sangat rendah. c. Karakteristik organisasi bank sangat memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank sangat baik. Lokasi operasional bank sangat terbatas. d. Frekuensi dan materialitas serangan siber bank selama 12 (dua belas) bulan terakhir sangat rendah dan tidak signifikan.
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 datang. Contoh karakteristik bank yang termasuk dalam peringkat *Low to Moderate* (2) antara lain sebagai berikut: a. Bank menggunakan teknologi informasi yang terbatas. Kerentanan terhadap gangguan atau serangan rendah. Bank melakukan *outsourcing* teknologi informasi pada pihak ketiga dengan kompleksitas yang sangat rendah. b. Variasi produk bank yang disalurkan menggunakan teknologi dan/atau jaringan *online* dan *mobile* terbatas dengan volume transaksi yang rendah. c. Karakteristik organisasi bank memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank baik. Lokasi operasional bank terbatas. d. Frekuensi dan materialitas serangan siber bank selama 12 (dua belas) bulan terakhir relatif rendah dan tidak signifikan.
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 datang. Contoh karakteristik bank yang termasuk dalam peringkat *Moderate* (3) antara lain sebagai berikut: a. Bank menggunakan teknologi informasi yang cukup terbatas. Kerentanan terhadap gangguan atau serangan cukup rendah. Bank melakukan *outsourcing* teknologi informasi pada pihak ketiga dengan kompleksitas yang rendah. b. Variasi produk bank yang disalurkan menggunakan teknologi dan/atau jaringan *online* dan *mobile* cukup terbatas dengan volume transaksi yang cukup rendah. c. Karakteristik organisasi bank cukup memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank cukup baik. Lokasi operasional bank cukup terbatas.

	d. Frekuensi dan materialitas serangan siber bank selama 12 (dua belas) bulan terakhir rendah namun cukup signifikan.
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 datang. Contoh karakteristik bank yang termasuk dalam peringkat *Moderate to High* (4) antara lain sebagai berikut: a. Bank menggunakan teknologi informasi yang kompleks dalam hal cakupan dan kecanggihannya. Kerentanan terhadap gangguan atau serangan cukup tinggi. Bank melakukan *outsourcing* teknologi informasi kritis pada pihak ketiga dengan kompleksitas yang cukup tinggi. b. Variasi produk bank yang disalurkan menggunakan teknologi dan/atau jaringan *online* dan *mobile* cukup tinggi dengan volume transaksi yang cukup tinggi. c. Karakteristik organisasi bank kurang memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank kurang baik dan kurang mapan. Lokasi operasional bank cukup beragam. d. Frekuensi dan materialitas serangan siber bank selama 12 (dua belas) bulan terakhir cukup tinggi dengan dampak yang cukup signifikan.
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 datang. Contoh karakteristik bank yang termasuk dalam peringkat *High* (5) antara lain sebagai berikut: a. Bank menggunakan teknologi informasi yang sangat kompleks dalam hal cakupan dan kecanggihannya. Kerentanan terhadap gangguan atau serangan sangat tinggi. Bank melakukan *outsourcing* teknologi informasi kritis pada pihak ketiga dengan kompleksitas yang tinggi. e. Variasi produk bank yang disalurkan menggunakan teknologi dan/atau jaringan *online* dan *mobile* sangat tinggi dengan volume transaksi yang sangat tinggi. b. Karakteristik organisasi bank tidak memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank tidak baik dan tidak mapan. Lokasi operasional bank sangat beragam. c. Frekuensi dan materialitas serangan siber bank selama 12 (dua belas) bulan terakhir sangat tinggi dengan dampak yang sangat signifikan.

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) antara lain sebagai berikut: a. Pengawasan aktif Direksi dan Dewan Komisaris secara keseluruhan sangat memadai. b. Sumber daya manusia sangat memadai 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 yang sangat baik mengenai manajemen risiko terkait keamanan siber. 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 sumber daya manusia 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 dan sangat sesuai dengan sasaran strategis dan strategi bisnis Bank. h. Strategi manajemen risiko terkait keamanan siber sangat sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko 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 internal dan fungsi yang melakukan kaji ulang independen sangat memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris. 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) antara lain sebagai berikut:

	a. Pengawasan aktif Direksi dan Dewan Komisaris secara keseluruhan memadai. b. Sumber daya manusia 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 yang baik mengenai manajemen risiko terkait keamanan siber. e. Budaya dan kesadaran manajemen risiko terkait keamanan siber telah dikembangkan dan diimplementasikan dengan baik di seluruh lingkungan organisasi Bank. f. Program peningkatan kapasitas sumber daya manusia 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 dan sesuai dengan sasaran strategis dan strategi bisnis Bank. h. Strategi manajemen risiko terkait keamanan siber sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko 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 internal dan fungsi yang melakukan kaji ulang independen memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris. n. Terdapat kelemahan yang tidak signifikan berdasarkan hasil kaji ulang independen. 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) antara lain sebagai berikut: a. Pengawasan aktif Direksi dan Dewan Komisaris secara keseluruhan cukup memadai. b. Sumber daya manusia 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 yang cukup baik mengenai manajemen risiko terkait keamanan siber. 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 sumber daya manusia 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 dan toleransi risiko 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 internal dan fungsi yang melakukan kaji ulang independen 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. 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) antara lain sebagai berikut: a. Pengawasan aktif Direksi dan Dewan Komisaris secara keseluruhan kurang memadai. Terdapat kelemahan pada berbagai aspek penilaian yang memerlukan perbaikan segera b. Sumber daya manusia kurang memadai 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 pada 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 sumber daya manusia 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 dan tidak sesuai dengan sasaran strategis dan strategi bisnis Bank. h. Strategi manajemen risiko terkait keamanan siber kurang sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko 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 yang komprehensif dan terintegrasi 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 internal dan fungsi yang melakukan kaji ulang independen kurang memadai, baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Direksi dan Dewan Komisaris. 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) antara lain sebagai berikut: a. Pengawasan aktif Direksi dan Dewan Komisaris secara tidak memadai. Terdapat kelemahan pada hampir seluruh aspek penilaian dan tindakan penyelesaiannya di luar kemampuan Bank. b. Sumber daya manusia tidak memadai 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 sangat lemah mengenai manajemen risiko terkait keamanan siber. 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 sumber daya manusia 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 dan 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 dan toleransi risiko 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 internal dan fungsi yang melakukan kaji ulang independen tidak memadai. Terdapat kelemahan pada metodologi, frekuensi, dan/atau pelaporan kepada Direksi dan Dewan Komisaris yang memerlukan perbaikan fundamental. 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 untuk menjaga 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) antara lain sebagai berikut: a. Proses identifikasi aset, ancaman dan kerentanan sangat memadai. b. Proses perlindungan 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 untuk menjaga 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) antara lain sebagai berikut: a. Proses identifikasi aset, ancaman, dan kerentanan memadai. b. Proses perlindungan 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 untuk menjaga ketahanan Siber cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen. Contoh karakteristik Bank yang termasuk dalam peringkat *Fair* (3) antara lain sebagai berikut: a. Proses identifikasi aset, ancaman, dan kerentanan cukup memadai. b. Proses perlindungan 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 untuk menjaga 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) ini antara lain sebagai berikut: 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. d. Proses penanggulangan dan pemulihan insiden siber dilaksanakan dengan kurang baik dan menimbulkan gangguan yang signifikan.
Unsatisfactory (5)	Kualitas penerapan proses untuk menjaga 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) ini antara lain sebagai berikut:

	a. Proses identifikasi aset, ancaman, dan kerentanan tidak memadai. b. Proses perlindungan 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 sehingga dinilai sangat mampu menghadapi insiden siber, 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 sehingga dinilai mampu menghadapi insiden siber, 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 sehingga dinilai cukup mampu menghadapi insiden siber, 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 sehingga dinilai kurang mampu menghadapi insiden siber, 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 sehingga dinilai tidak mampu menghadapi insiden siber, 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.

LAMPIRAN IV

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR ...

TENTANG

KETAHANAN DAN KEAMANAN SIBER BAGI BANK UMUM

IV.a Format Notifikasi Awal Insiden Siber

NOTIFIKASI AWAL INSIDEN SIBER

A. INFORMASI PELAPOR

Nama Bank : .....
Alamat Kantor Pusat Bank : .....
Nomor Telepon : .....

Nama Pelapor : .....
Kantor/Divisi/Bagian Pelapor : .....
Alamat Pelapor : .....
Nomor Telepon Pelapor : .....

Tanggal Penyampaian Notifikasi : .....

Otoritas/Lembaga Penerima : .....[1)]

B. INFORMASI UMUM INSIDEN SIBER

1. Tanggal Terjadinya Insiden Siber : ..../..../..... (dd/mm/yyyy)
2. Waktu Insiden Siber Diketahui : ... : .... (hh:mm)
3. Jenis Insiden Siber : .....[2)]
4. Titik Serangan : .....[3)]
5. Respon Awal Bank Pasca Insiden Siber:[4)]
   .....

C. PENILAIAN AWAL ATAS DAMPAK INSIDEN SIBER BAGI BANK

1. Penilaian Dampak Insiden Siber terhadap Bisnis Bank[5)] .....
2. Penilaian Dampak Insiden Siber terhadap Pihak Ketiga[6)] .....
3. Penilaian Dampak Finansial dari Insiden[7)] .....
4. Penilaian Dampak terhadap Reputasi Bank[8)] .....
5. Penilaian Dampak terhadap Aspek Hukum dan Kepatuhan[9)] .....
6. Penilaian Dampak lainnya yang dapat Diidentifikasi oleh Bank .....

Keterangan:

1) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima pelaporan notifikasi awal ini (jika ada).
2) Memuat informasi mengenai jenis insiden siber. Contoh: *Malware*, *Hacking*, *Ransomware*, *Web Defacement*, *Denial of Services* (DoS)/*Distributed Denial of Services* (DDoS).
3) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
4) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden siber.

5) 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,* pembiayaan perdagangan, *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).
6) 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)
7) 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 mitra terdampak)
8) Diisi dalam hal terdapat dampak terhadap reputasi Bank dari insiden siber (contoh potensi insiden siber menarik perhatian media).
9) Diisi dalam hal terdapat dampak terhadap aspek hukum dan kepatuhan, (contoh potensi pelanggaran ketentuan peraturan perundang-undangan dan potensi adanya tuntutan hukum dari pihak terkait).

IV.b Format Laporan Insiden Siber

LAPORAN INSIDEN SIBER

A. INFORMASI PELAPOR

Nama Bank : .....
Alamat Kantor Pusat Bank : .....
Nomor Telepon : .....

Nama Pelapor : .....
Kantor/Divisi/Bagian Pelapor : .....
Alamat Pelapor : .....
Nomor Telepon Pelapor : .....

Tanggal Penyampaian Notifikasi Awal: .....
Tanggal Laporan Insiden Siber: .....

B. INFORMASI UMUM INSIDEN SIBER[1)]

1. Tanggal Terjadinya Insiden Siber : ..../..../..... (dd/mm/yyyy)
2. Waktu Insiden Siber Diketahui : ... : .... (hh:mm)
3. Jenis Insiden Siber : ..... [2)]
4. Titik Serangan : ..... [3)]
5. Respon Awal Bank Pasca Insiden Siber: [4)]
   .....

C. PENILAIAN ATAS DAMPAK INSIDEN SIBER BAGI BANK[5)]

1. Penilaian Dampak Insiden Siber terhadap Bisnis Bank[6)] .....
2. Penilaian Dampak Insiden Siber terhadap Pihak Ketiga[7)] .....
3. Penilaian Dampak Finansial dari Insiden[8)] .....
4. Penilaian Dampak terhadap Reputasi Bank[9)] .....
5. Penilaian Dampak terhadap Aspek Hukum dan Kepatuhan[10)] .....
6. Penilaian Dampak lainnya 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-pihak yang menerima informasi terkait siber (*stakeholder* terkait, contoh: otoritas, mitra layanan, dan nasabah)

E. ANALISIS PENYEBAB TERJADINYA INSIDEN

1. Sumber Serangan:
   a. Pihak : ..... [11)]
   b. Negara Asal : ..... [12)]
   c. Motif Serangan : ..... [13)]
2. Faktor penyebab insiden: ..... [14)]

F. ANALISIS FINAL

1. Kesimpulan.
2. Langkah Perbaikan.[15)]
3. Target Waktu Penyelesaian Insiden Siber : ..... (dd/mm/yy) [16)]

Keterangan:

1) Berisi informasi yang sesuai dengan informasi yang telah disampaikan pada notifikasi awal, namun dapat ditambahkan atau disesuaikan dengan informasi tambahan bila ada.
2) Memuat informasi mengenai jenis insiden siber. Contoh: *Malware*, *Hacking*, *Ransomware*, *Web Defacement*, *Denial of Services* (DoS)/*Distributed Denial of Services* (DDoS).
3) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
4) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden siber.
5) Pada bagian ini informasi yang diberikan berupa penjelasan tambahan dari penilaian awal yang sudah dilakukan oleh Bank saat pelaporan notifikasi awal insiden siber.
6) 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*, pembiayaan perdagangan, *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).
7) 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).
8) 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 mitra terdampak).
9) Diisi dalam hal terdapat dampak terhadap reputasi Bank dari insiden siber, contoh potensi insiden menarik perhatian media.

10) Diisi dalam hal terdapat dampak terhadap aspek hukum dan kepatuhan, contoh potensi pelanggaran ketentuan peraturan perundang-undangan dan potensi adanya tuntutan hukum dari pihak terkait.
11) Memuat informasi mengenai pihak yang melakukan serangan atau menjadi sumber serangan, antara lain: pihak internal, pihak eksternal atau pihak ketiga, apabila dapat diketahui.
12) Memuat informasi mengenai negara asal dari sumber serangan, apabila dapat diketahui.
13) Memuat informasi mengenai motif atau tujuan atas serangan yang dilakukan oleh pihak, apabila dapat diketahui.
14) Memuat penjelasan lengkap dari faktor-faktor yang menyebabkan terjadinya insiden siber di Bank.
15) Memuat informasi mengenai langkah-langkah yang dilakukan Bank untuk mencegah insiden serupa terjadi di masa mendatang.
16) Diisi dalam hal insiden belum sepenuhnya diselesaikan pada saat menyampaikan laporan kepada Otoritas Jasa Keuangan.

LAMPIRAN V

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR ...

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		

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		

Tingkat Risiko terkait Keamanan Siber	

Analisis

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.