CONSULTATIVE PAPER

Manaiemen Risiko Keamanan Siber Bank Umum

Departemen Penelitian dan Pengaturan Perbankan
Otoritas Jasa Keuangan - 2021

halaman ini sengaja dikosongkan

Daftar Isi

I. Pendahuluan **4**

II. Ruang Lingkup **6**

III. Konsep Dasar Keamanan Siber **7**

IV. Standar Penerapan Manajemen Risiko Keamanan Siber **13**

A. Risiko Inheren Keamanan Siber **13**

B. Aspek Manajemen Risiko Keamanan Siber **15**

B.1. Tata Kelola Risiko Keamanan Siber 15

B.2. Kerangka Manajemen Risiko Keamanan Siber 24

B.3. Proses Identifikasi, Perlindungan, Ketanggapan, dan Ketahanan serta Sistem Informasi Manajemen Risiko Keamanan Siber 29

B.4 Kecukupan Sistem Pengendalian Internal 46

V. Penilaian Tingkat Maturitas Manajemen Risiko Keamanan Siber **52**

VI. Pengujian Ketahanan Keamanan Siber **54**

VII. Pelaporan **56**

Lampiran A – Format Laporan Insiden Siber **59**

Lampiran B – Penilaian Tingkat Risiko Keamanan Siber Inheren **62**

Lampiran C – Penilaian Tingkat Kualitas Penerapan Manajemen Risiko Keamanan Siber Bank **66**

Lampiran D – Penilaian Tingkat Maturitas Manajemen Risiko Keamanan Siber Bank **74**

I. Pendahuluan

1. Perkembangan ekonomi digital dan inovasi di bidang Teknologi Informasi (TI) yang pesat memiliki dampak terhadap perkembangan pelayanan jasa di berbagai sektor, termasuk jasa perbankan. Perbankan dapat memanfaatkan berbagai inovasi TI untuk menyediakan produk dan jasa yang berkualitas serta lebih efisien bagi nasabah atau masyarakat. Namun demikian, perkembangan TI juga berdampak pada semakin meningkatnya risiko terkait teknologi bagi Bank.
2. Selama beberapa tahun terakhir, risiko dari ancaman dan insiden siber telah muncul sebagai isu yang berkembang di sektor perbankan. Sejak awal pandemi Covid-19, ancaman dan insiden siber semakin meningkat terutama didukung dengan semakin maraknya *remote working* dan peningkatan layanan keuangan digital sehingga memperbesar titik kerentanan untuk dapat masuk ke dalam sistem TI Bank.
3. Meningkatnya ancaman siber yang semakin canggih dan maraknya insiden siber menuntut kewaspadaan dan kemampuan Bank dalam menghadapi dan menangani ancaman yang muncul. Insiden siber yang tidak ditangani dengan baik dapat mengganggu proses bisnis perbankan yang akan berdampak secara luas. Selain itu, keamanan siber yang kurang memadai juga akan berdampak pada hilangnya kepercayaan terhadap Bank dan dapat menimbulkan risiko reputasi yang cukup substansial.
4. Maraknya serangan siber telah mendorong kebutuhan untuk meningkatkan ketahanan siber (*cyber resilience*) melalui penguatan manajemen risiko keamanan siber (*cyber security risk management*). Regulator perbankan di berbagai negara mulai melihat pentingnya penerapan manajemen risiko keamanan siber untuk mengatasi ancaman risiko siber (*cyber risk*). Terlebih lagi, perbankan merupakan sektor yang menjadi target serangan siber paling tinggi baik secara global maupun di Indonesia.

5. Sehubungan dengan hal tersebut, Basel Committee on Banking Supervision (BCBS) meminta agar seluruh otoritas perbankan mendorong Bank untuk menerapkan manajamen risiko keamanan siber yang efektif. Bank diharapkan memiliki kebijakan manajemen risiko keamanan siber serta mampu mengidentifikasi, melindungi, mendeteksi, merespon, dan mengatasi ancaman risiko siber dengan lebih baik sehingga memiliki ketahanan yang lebih besar terhadap ancaman risiko siber sebagai implementasi manajemen risiko operasional dan ketahanan operasional Bank.
6. Berdasarkan catatan dari Bank for International Settlements (BIS), otoritas perbankan di beberapa negara telah memiliki kebijakan khusus terkait manajemen risiko keamanan siber. Beberapa *best practices* di berbagai negara yang bertujuan untuk meningkatkan manajemen risiko keamanan siber antara lain mencakup kebijakan terkait pengelolaan keamanan siber, kewajiban penilaian risiko keamanan siber, kewajiban pengujian kerentanan TI Bank, penilaian tingkat maturitas manajemen risiko keamanan siber, dan pelaksanaan pengujian keamanan siber Bank. *Best practices* tersebut perlu diimplementasikan pada perbankan Indonesia agar Bank mampu melakukan mitigasi ancaman risiko keamanan siber.
7. BCBS merekomendasikan beberapa standar internasional dan *best practices* terkait keamanan siber yang dapat dijadikan sebagai acuan antara lain National Institute of Standards and Technology (NIST) Framework for Improving Cyber Security, NIST Risk Management Framework, ISO 27001 – Information Security Management Standard, ISO 27032 – Guidelines for Cybersecurity, dan Financial Stability Board (FSB) Cyber Incident Response and Recovery Toolkits.
8. Mengingat tingginya dampak digitalisasi terhadap keamanan siber Bank, diperlukan suatu kerangka pengaturan manajemen risiko keamanan siber di sektor perbankan untuk melengkapi kebijakan terkait manajemen risiko teknologi informasi bagi bank umum yang sebelumnya telah diatur dalam

POJK Nomor 38/POJK.03/2016 sebagaimana telah diubah dengan POJK Nomor 13/POJK.03/2020 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum dan SEOJK Nomor 21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum serta POJK Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum.

9. *Consultative paper* ini berisikan arah pengaturan manajemen risiko keamanan siber bagi Bank Umum dan diterbitkan untuk memperoleh masukan dari berbagai pihak. Masukan dari berbagai pihak atas *consultative paper* ini diharapkan dapat disampaikan paling lambat 30 Februari 2022.

II. Ruang Lingkup

10. Bank harus menerapkan manajemen risiko keamanan siber secara efektif. Bank dalam hal ini adalah bank umum sebagaimana dimaksud dalam Undang-Undang Nomor 7 tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998, termasuk kantor cabang dari bank yang berkedudukan di luar negeri.
11. Dalam menerapkan manajemen risiko keamanan siber, Bank harus memperhatikan peraturan perundang-undangan yang berlaku terkait keamanan siber.
12. Penerapan manajemen risiko keamanan siber harus disesuaikan dengan tujuan, kebijakan usaha, ukuran dan kompleksitas usaha, teknologi informasi yang digunakan, serta kemampuan Bank.
13. *Consultative paper* ini berisikan standar minimal yang harus dipenuhi oleh Bank dalam menerapkan manajemen risiko keamanan siber. *Consultative paper* ini memuat konsep dasar keamanan siber, uraian mengenai standar penerapan manajemen risiko keamanan siber, penilaian tingkat maturitas

manajemen risiko keamanan siber, pengujian pertahanan keamanan siber, dan pelaporan penerapan manajemen risiko keamanan siber.

III. Konsep Dasar Keamanan Siber

14. Keamanan siber *(cybersecurity)* didefinisikan sebagai terjaganya kerahasiaan, keutuhan dan ketersediaan informasi dan/atau sistem informasi melalui media siber. Keamanan siber meliputi pula hal-hal antara lain keaslian *(authenticity)*, akuntabilitas, non-penyangkalan *(non-repudiation)*, dan keandalan.[1] Adapun ruang siber adalah ruang dimana komunitas saling terhubung dengan menggunakan jaringan untuk melakukan berbagai kegiatan.[2] Ruang siber juga dapat digambarkan sebagai lingkungan atau ruang virtual yang dihasilkan oleh adanya jaringan internet, termasuk *people,* organisasi, dan kegiatan yang terkait pada perangkat teknologi dan jaringan yang terhubung dengan ruang siber tersebut.[3]
15. Risiko keamanan *siber* adalah kombinasi kemungkinan terjadinya insiden di dalam ranah aset dan informasi, atau sumber daya teknologi dan komunikasi serta dampak dari insiden tersebut bagi suatu organisasi.[4] Insiden siber adalah

---

[1] Definisi *cyber security* berdasarkan FSB *Cyber Lexicon* (*https://www.fsb.org/wp-content/uploads/P121118-1.pdf*). Diadaptasi dari International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27032:2012 – *Guidelines for cybersecurity.*

[2] Definisi ruang siber berdasarkan Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

[3] Definisi ruang siber berdasarkan ISO/IEC 27032 *Guidelines for Cybersecurity,*

[4] Definisi *cyber risk* berdasarkan FSB *Cyber Lexicon* (*https://www.fsb.org/wp-content/uploads/P121118-1.pdf*). Untuk mendukung *international standard setting bodies*, regulator, pelaku usaha, dan organisasi internasional di sektor jasa keuangan dalam menangani *financial cyber resilience*, pada tahun 2018 Financial Stability Board (FSB) telah menyusun *Cyber Lexicon*. Lexicon ini terdiri dari kurang lebih 50 (lima puluh) istilah inti yang terkait dengan *cyber security* dan *cyber resilience* di sektor keuangan yang dapat digunakan untuk memberikan kesepahaman terminologi di bidang siber. Definisi *cyber risk* diadaptasi dari CPMI – IOSCO (*Committee on Payments and Market Infrastructures – International Organization of Securities Commissions*), ISACA (*Information Systems Audit and Control Association*) Fundamentals, dan ISACA *Full Glossary.*

kejadian di ruang siber yang (i) membahayakan keamanan siber dari sistem informasi atau (ii) melanggar kebijakan dan prosedur keamanan, baik yang dihasilkan dari aktivitas berbahaya ataupun bukan.[5] Adapun kejahatan siber merupakan perilaku ilegal yang dikendalikan melalui operasi elektronik yang menjadikan sistem keamanan komputer dan data yang diproses sebagai targetnya.

16. Sumber risiko keamanan siber dapat berasal dari pihak internal (sumber daya manusia, proses, dan sistem) maupun faktor eksternal Bank, dengan penjelasan sebagai berikut:

    a. Sumber Daya Manusia (SDM)

       SDM merupakan sumber dari risiko 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.

    b. Proses

       Desain dan implementasi proses bisnis dalam Bank dapat menyebabkan terjadinya risiko siber bagi Bank. Kelemahaan 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.

    c. Sistem

       Kelemahan pada teknologi informasi dan infrastruktur Bank dapat menjadi sumber risiko siber. Kurangnya pengujian pengamanan, kontrol, dan monitoring ancaman dan kerentanan, kelemahan sistem, seperti tidak

[5] Definisi insiden siber diadaptasi dari NIST (*National Institute of Standards and Technology*). Berdasarkan definisi dimaksud, insiden siber sendiri memiliki pengertian yang lebih luas dan mencakup seluruh peristiwa terkait siber yang tidak terbatas pada kejahatan saja.

tersedianya *anti malware/ anti virus,* dan sistem yang tidak *update* menjadi jalan bagi masuknya risiko siber kepada Bank.

d. 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.

17. Ancaman keamanan siber dapat terjadi dalam berbagai bentuk. Bentuk-bentuk serangan yang mengancam keamanan siber meliputi antara lain:

a. Penyusupan (*intrusion*) yaitu masuknya penyerobot pada sistem dan aplikasi Bank tanpa seijin dan sepengetahuan dari Bank, dan berusaha mengubah sistem dari Bank. Penyusupan dapat menyerang sistem melalui identifikasi pengguna yang sah dan parameter koneksi seperti sandi (*password*), melalui eksploitasi kerentanan yang ada pada sistem dan aplikasi. Metode utama yang digunakan untuk mendapatkan akses ke dalam sistem dan aplikasi antara lain menebak sandi yang digunakan (*brute force*), mengakses akun yang tidak dilindungi dengan sandi, melakukan penipuan atau rekayasa social, mendengarkan lalu lintas komunikasi data dengan alat penyadap, memasukan program mata-mata (*spyware*) atau program kecil yang umumnya digunakan sebagai pengganti diri untuk masuk (login) ke dalam sistem dan aplikasi (*trojan horse*), mengakses file yang menyimpan semua sandi pengguna yang dienkripsi untuk kemudian dibuka dengan utilitas yang tersedia pada jaringan, dan menguji semua permutasi yang mungkin untuk memecahkan sandi (*cracking password*)

b. Serangan *Phishing*, dilakukan dengan cara memberikan alamat *website* palsu dengan tampilan persis sama dengan *website* aslinya. Tujuan dari serangan *phishing* ini adalah untuk mendapatkan informasi penting dan sensitif seperti *username*, *password* dan lain-lain.

c. Serangan *Malware*, yaitu suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer. Biasanya program *malware* telah dirancang untuk mendapatkan keuntungan finansial atau keuntungan lain yang direncanakan. Jumlah serangan malware terus berkembang, sehingga saat ini telah menjadi pandemi yang sangat nyata. *Malware* telah terjadi dimana-mana dan mempengaruhi semua orang yang terlibat dalam setiap sektor kegiatan. Istilah virus generik digunakan untuk merujuk setiap program komputer berbahaya yang mampu mereproduksi dan menyebarkan dirinya sendiri.

d. *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), biasanya dilakukan dengan melakukan overloading kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Sehingga sistem menjadi terlalu sibuk dan crash, akibatnya menjadi tidak dapat melayani atau tidak dapat beroperasi. Permasalahan ini merupakan ancaman yang berbahaya bagi Bank yang mengandalkan hampir sepenuhnya pada kemampuan internet guna menjalankan roda kegiatannya.

e. Serangan *Defacement*, dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web korban sehingga isi dari halaman web korban berubah sesuai dengan motif penyerang.

f. Serangan *spam* yang dilakukan dengan cara mengirimkan email yang tidak dikehendaki dengan tujuan komersial atau publisitas, memperkenalkan perangkat lunak berbahaya, atau menyebabkan server menjadi penuh dan kelebihan beban.

g. Penyalahgunaan Protokol Komunikasi. Sebuah serangan *spoofing Transmision Control Protocol* (TCP) bergantung pada kenyataan bahwa protokol TCP menetapkan koneksi logis antara dua ujung sistem untuk mendukung pertukaran data. Pengidentifikasi logis (nomor port) digunakan untuk membangun sebuah koneksi TCP. Sebuah serangan TCP nomor port akan melibatkan kegiatan menebak atau memprediksi nomor port berikutnya yang akan dialokasikan untuk pertukaran data dalam rangka menggunakan angka-angka bukan pengguna yang sah. Hal ini memungkinkan untuk melewati firewall dan mendirikan sebuah hubungan yang aman antara dua entitas, yaitu *hacker* dan target.

h. *Social engineering,* yaitu tindakan memperoleh informasi nasabah seperti PIN, nomor baru, dan/atau informasi lain dengan cara menghubungi nasabah melalui telepon, SMS, atau media lain untuk menyampaikan informasi tertentu agar nasabah menghubungi nomor tertentu atau membuka situs web tertentu.

i. *Business email compromise,* merupakan kejahatan siber *social engineering* yang memanfaatkan celah kerentanan dari sebuah surat elektronik (*email*) yag menargetkan organisasi bisnis, professional, dan individu dengan mengorbankan salah satu bisnis atau akun *email* pribadi untuk mengirim (atau menyebabkan dikirim) instruksi pembayaran palsu dan informasi lain yang digunakan untuk melakukan penipuan keuangan.

18. Secara umum, jenis ancaman keamanan siber dapat dikelompokan menjadi 3 (tiga) sebagai berikut:[6]

a. Ancaman Perangkat Keras (*hardware threat*), yaitu ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tsb

[6] Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

merupakan gangguan terhadap sistem Jaringan dan Perangkat Keras lainnya, contoh: *Jamming*[7] dan *Network Intrusion*.

b. Ancaman Perangkat Lunak (software threat), yaitu ancaman yang disebabkan oleh masuknya software tertentu yang berfungsi untuk melakukan kegiatan seperti: Pencurian Informasi (*Information Theft*), Perusakan Informasi/Sistem (*Information/System Destruction*), Manipulasi Informasi (*Information Corruption*) dan lain sebagainya, ke dalam suatu sistem.

c. Ancaman Data/Informasi (*data/information threat*), adalah ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam information *warfare* termasuk kegiatan propaganda.

19. Berbagai kejadian risiko keamanan siber dapat menyebabkan dampak terhadap Bank antara lain sebagai berikut:

a. Kerugian Langsung

Kerugian langsung adalah kerugian yang dapat dihitung dan berdampak langsung pada Bank, contohnya kehilangan aset dan pembayaran ganti rugi kepada pihak lain (nasabah).

b. Kerugian Tidak Langsung

Kerugian tidak langsung adalah kerugian yang sulit dihitung secara kuantitatif, namun dapat mengurangi efektivitas dari efisiensi bisnis Bank. Contoh dari kerugian tidak langsung adalah inefisiensi proses kerja, kehilangan kesempatan untuk memperoleh klaim/ keuntungan, dan kehilangan atau berkurangnya kepercayaan masyarakat terhadap Bank.

20. Sebagaimana tujuan dari manajemen risiko operasional adalah *operational* resilience*,* maka tujuan dari manajemen risiko keamanan siber adalah *cyber*

[7] *Jamming* adalah jenis serangan yang bertujuan untuk mengganggu penerimaan sinyal atau komunikasi. (NIST *Computer Security Resource Center*)

resilience. Cyber resilience[8] diartikan sebagai kemampuan Bank untuk terus beroperasi dengan mengantisipasi dan beradaptasi dengan ancaman siber[9], yaitu suatu keadaan yang berpotensi mengeksploitasi satu atau lebih kerentanan yang berdampak buruk pada keamanan siber, dan perubahan lain yang relevan, serta kemampuan bertahan, menahan, dan pulih dengan cepat dari insiden siber.

IV. Standar Penerapan Manajemen Risiko Keamanan Siber

21. Bank harus secara proaktif menerapkan manajemen risiko keamanan siber untuk memastikan keberlangsungan operasional aktivitasnya. Dalam hal ini, Bank perlu memperhatikan risiko inheren dari keamanan siber dan aspek manajemen risiko keamanan siber.

A. Risiko Inheren Keamanan Siber

22. Bank harus melakukan identifikasi atas risiko inheren keamanan siber. Risiko inheren tersebut meliputi risiko yang dapat dikuantifikasi maupun yang tidak dapat dikuantifikasi yang berpotensi mempengaruhi kegiatan operasional Bank. Karakteristik risiko inheren tersebut sangat ditentukan oleh faktor internal maupun eksternal, antara lain strategi bisnis, karakteristik bisnis, teknologi informasi yang dipergunakan oleh Bank, kompleksitas produk dan aktivitas Bank, dan ancaman keamanan siber yang terjadi.

---

[8] Definisi *cyber resilience* berdasarkan FSB *Cyber Lexicon (https://www.fsb.org/wp-content/uploads/P121118-1.pdf).* Diadaptasi dari Carnegie Mellon Software Engineering Institute, CERT® Resilience Management Model, Version 1.2, Glossary of Terms (https://resources.sei.cmu.edu/asset_files/BookChapter/2016_009_001_514934.pdf), CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (June 2016) (https://www.bis.org/cpmi/publ/d146.pdf), dan NIST, Glossary of Key Information Security Terms, Revision 2 (May 2013) (https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

[9] Definisi *cyber threat* berdasarkan FSB *Cyber Lexicon* (*https://www.fsb.org/wp-content/uploads/P121118-1.pdf).* Diadaptasi dari CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (June 2016) (https://www.bis.org/cpmi/publ/d146.pdf)

23. Penilaian risiko inheren dilakukan dengan memperhatikan paling sedikit 5 (lima) faktor penilaian, yaitu teknologi, saluran distribusi, produk dan aktivitas, karakter organisasi, dan *track record* ancaman siber[10]. Penilaian risiko inheren diawali dari penilaian terhadap parameter risiko pada setiap faktor risiko siber.

a) Teknologi

Jenis teknologi yang berbagai macam yang digunakan oleh Bank dapat menimbulkan berbagai tingkat risiko yang melekat pada Bank, tergantung pada pada kompleksitas dan tingkat kematangan Bank. Untuk menentukan risiko inheren atau risiko yang melekat dalam kategori teknologi, diperlukan pertimbangan terhadap beberapa hal sebagai berikut: keseluruhan infrastruktur teknologi dan informasi (TI), seperti jumlah *internet service provider,* dan koneksi pihak ketiga, penyelenggaraan sistem teknologi informasi, jumlah koneksi yang tidak aman (*unsecured connection*), penggunaan akses nirkabel, jumlah perangkat jaringan, penggunaan *cloud* dan teknologi terkini lainnya (*emerging techonolgies*).

b) Saluran Distribusi (*Delivery Channel*)

Perbedaan *delivery channel* untuk produk dan aktivitas Bank dapat memberikan risiko yang berbeda bagi Bank. Risiko inheren Bank pada umumnya akan meningkat seiring dengan jenis, jumlah, dan tingkat kompleksitas *delivery channel* yang digunakan. Sebagai contoh, risiko inheren yang lebih tinggi akan dihasilkan untuk produk dan aktivitas Bank yang menggunakan jalur *online* dan *mobile,* serta mekanisme pengelolaan *automated teller machine* (ATM), misalnya *joint* ATM *network,* pengelolaan oleh pihak ketiga, atau pengelolaan secara mandiri).

c) Produk, Layanan, dan Jasa

---

10 *Federal Financial Institutions Examination Council, Cybersecurity Assessment Tools (https://www.ffiec.gov/cyberassessmenttool.htm)*

Perbedaan jenis produk, layanan, dan/atau jasa terkait teknologi yang diberikan oleh Bank dapat memberikan risiko inheren yang berbeda tergantung kompleksitas produk dan layanan diberikan. Kategori ini antara lain dapat mencakup berbagai layanan pembayaran serta pertimbangan penyediaan layanan teknologi oleh Bank.

d) Karakter Organisasi

Kategori ini mempertimbangkan karakteristik organisasi bank yang juga dapat memberikan dampak terhadap risiko inheren bank, antara lain dalam hal jumlah pegawai, IT *control environment,* kedudukan atau lokasi operasional.

e) *Track Record* Ancaman Siber

Volume dan jenis serangan siber, baik percobaan serangan atau serangan yang berhasil dilakukan, mempengaruhi eksposur risiko yang melekat pada Bank. Kategori ini mempertimbangkan volume dan kecanggihan serangan yang menargetkan Bank sebagai sasaran.

B. Aspek Manajemen Risiko Keamanan Siber

24. Bank harus menerapkan aspek manajemen risiko keamanan siber yang paling sedikit mencakup (i) tata kelola, (ii) strategi, (iii) perlindungan, ketanggapan, ketahanan, dan (iv) sistem pengendalian internal.

B.1. Tata Kelola Risiko Keamanan Siber

25. Tata kelola risiko keamanan siber mencakup (i) pengawasan aktif Direksi dan Dewan Komisaris, (ii) struktur organisasi; (iii) sumber daya manusia; (iv) budaya dan kesadaran, dan (v) peningkatan kapasitas.

B.1.1. Pengawasan Aktif Direksi dan Dewan Komisaris

26. Bank harus menetapkan wewenang dan tanggung jawab yang jelas pada setiap jenjang jabatan yang terkait dengan penerapan manajemen risiko

keamanan siber. Hal ini termasuk wewenang dan tanggung jawab terkait pengawasan aktif oleh Direksi dan Dewan Komisaris.

27. Wewenang dan tanggung jawab Direksi dan Dewan Komisaris paling sedikit meliputi:
    a. Memiliki tanggung jawab penuh atas penerapan manajemen risiko keamanan siber Bank.
    b. Bertanggung jawab untuk memastikan penerapan manajemen risiko keamanan siber telah memadai sesuai dengan karakteristik, kompleksitas, dan profil risiko Bank.
    c. Memiliki pemahaman yang memadai mengenai jenis dan tingkat risiko keamanan siber yang melekat pada Bank.
    d. Memastikan Bank memiliki sumber daya manusia dan infrastruktur yang cukup untuk mendukung manajemen risiko keamanan siber Bank.
    e. Mendukung terciptanya budaya manajemen risiko keamanan siber dengen memberikan perhatian yang cukup terhadap pelaksanaan manajemen risiko keamanan siber oleh seluruh elemen organisasi Bank.
    f. Menjadi contoh standar perilaku yang mengedepankan kesadaran terhadap risiko siber bagi pegawai dan seluruh elemen organisasi Bank.
    g. Melakukan pengawasan secara aktif atas penerapan manajemen risiko keamanan siber.
28. Wewenang dan tanggung jawab Dewan Komisaris, paling sedikit meliputi:
    a. menyetujui kebijakan dan rencana strategis terkait manajemen risiko keamanan siber yang ditetapkan sesuai dengan tingkat risiko yang akan diambil dan toleransi risiko Bank;
    b. mengevaluasi kebijakan manajemen risiko dan strategi risiko 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;

c. mengevaluasi pertanggungjawaban Direksi dan memberikan arahan perbaikan atas pelaksanaan kebijakan manajemen risiko keamanan siber secara berkala; dan

d. memastikan kebijakan dan proses manajemen risiko keamanan siber dilaksanakan secara efektif dan terintegrasi dalam proses manajemen risiko secara keseluruhan.

29. Wewenang dan tanggung jawab Direksi, paling sedikit meliputi

a. menyusun dan menetapkan kebijakan, strategi, dan kerangka manajemen risiko keamanan siber secara tertulis dan kompehensif termasuk limit risiko keamanan siber dan melakukan pemantauan implementasi manajemen risiko keamanan siber oleh Bank;

b. menyusun, menetapkan, dan mengkinikan prosedur untuk mengidentifikasi, mengukur, memonitor, dan mengendalikan risiko siber;

c. melaksanakan kebjakan strategi dan kerangka manajemen risiko 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 keamanan siber, satuan kerja manajemen risiko, satuan kerja kepatuhan, dan satuan kerja audit internal;

d. mengevaluasi dan/atau mengkinikan kebijakan, strategi, dan kerangka manajemen risiko operasional dan melakukan internalisasi kerangka manajemen risiko siber ke dalam kebijakan dan prosedur bisnis pada seluruh unit bisnis dan aktivitas pendukung;

e. menetapkan struktur organisasi termasuk wewenang dan tanggung jawab yang jelas pada setiap jenjang jabatan yang terkait dengan penerapan manajemen risiko siber;

f. Memastikan kecukupan dukungan sumber daya untuk mengelola dan mengendalian risiko keamanan siber;

g. 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;

h. 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 keamanan siber dalam organisasi Bank;

i. 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;

j. memastikan seluruh risiko 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 pemasalahan terkait risiko keamanan siber yang material disertai dengan langkah-langkah perbaikan yang telah, sedang, dan akan dilakukan;

k. memastikan pelaksanaan langkah-langkah perbaikan atas permasalahan atau penyimpangan terkait keamanan siber yang ditemukan; dan

l. memastikan bahwa fungsi manajemen risiko keamanan siber telah diterapkan secara independen tercermin dari antara lain adanya pemisahan fungsi antara satuan kerja pelaksana dengan satuan kerja yang berfungsi untuk melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko keamanan siber.

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.

B.1.2. Sumber Daya Manusia

30. Direksi harus 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 keamanan siber, baik untuk unit bisnis, SKMR maupun unit pendukung yang bertanggung jawab atas pelaksanaan manajemen risiko keamanan siber.
31. Direksi harus 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 keamanan siber.
32. Direksi harus memastikan bahwa seluruh sumber daya manusia memiliki pemahaman yang memadai atas risiko keamanan siber dan mampu mengkomunikasikan implikasi risiko keamanan siber kepada Dewan Komisaris, Direksi, manajemen, dan nasabah.
33. Direksi harus memastikan agar seluruh sumber daya manusia memahami strategi, tingkat risiko keamanan siber yang akan diambil dan toleransi risiko keamanan siber, kerangka manajemen risiko keamanan siber yang telah ditetapkan Direksi dan disetujui oleh Dewan Komisaris serta memastikan seluruh sumber daya manusia menerapkan secara konsisten dalam aktivitas yang ditangani.
34. Bank harus meyakini telah memiliki integritas informasi meliputi pengetahuan, keterampilan, kemampuan dan karakter seluruh pegawai Bank, di antaranya dengan melakukan pemeriksaan latar belakang *(background check)* untuk karyawan baru, dalam rangka perlindungan stakeholder maupun reputasi Bank, serta mencegah potensi terjadinya aktivitas kriminal.

B.1.3. Struktur Organisasi

35. Direksi harus menetapkan struktur organisasi yang disertai dengan kejelasan dan tanggung jawab secara umum maupun terkait penerapan manajemen risiko keamanan siber pada seluruh satuan kerja yang disesuaikan dengan tujuan dan kebijakan usaha serta ukuran dan kompleksitas kegiatan usaha Bank.
36. Struktur organisasi harus dirancang untuk memastikan bahwa satuan kerja yang melakukan fungsi pengendalian intern terhadap manajemen risiko keamanan siber independen terhadap satuan kerja bisnis.
37. Direksi harus membentuk unit kerja atau fungsi yang bertugas menangani penerapan manajemen risiko keamanan siber dalam organisasi Bank.
38. Struktur unit kerja atau fungsi yang bertugas menangani penerapan manajemen risiko keamanan siber disesuaikan dengan ukuran dan kompleksitas kegiatan usaha Bank serta risiko keamanan siber Bank.
39. Pimpinan unit kerja atau fungsi yang bertugas menangani penerapan manajemen risiko keamanan siber bertanggung jawab kepada Direktur yang ditugaskan secara khusus untuk menangani keamanan siber.
40. Wewenang dan tanggung jawab unit kerja atau fungsi yang bertugas menangani penerapan manajemen risiko keamanan siber paling sedikit meliputi:
    a. memberikan masukan kepada Direksi dalam penyusunan kebijakan, strategi, dan kerangka manajemen risiko keamanan siber;
    b. mengembangkan prosedur dan alat untuk identifikasi, pengukuran, pemantauan, dan pengendalian risiko keamanan siber;
    c. mendesain dan menerapkan perangkat yang dibutuhkan dalam penerapan manajemen risiko keamanan siber;
    d. memantau implementasi kebijakan, strategi, dan kerangka manajemen risiko yang ditetapkan oleh Direksi dan telah disetujui oleh Dewan Komisaris;

e. memantau posisi atau eksposur risiko keamanan siber secara keseluruhan, termasuk pemantauan kepatuhan terhadap toleransi risiko keamanan siber dan limit yang ditetapkan;
f. melakukan pengujian ketahanan siber guna mengetahui dampak dari implementasi kebijakan dan strategi manajemen risiko keamanan siber terhadap profil risiko Bank secara keseluruhan;
g. mengkaji usulan produk dan/atau aktivitas baru dan penggunaan teknologi baru yang dikembangkan oleh suatu unit tertentu Bank yang difokuskan terutama pada dampak dari produk dan/aktivas baru dan penggunaan terknologi baru tersebut terhadap eksposur risiko keamanan siber Bank secara keseluruhan;
h. memberikan rekomendasi kepada Direksi dan/atau satuan kerja terkait penerapan manajemen risiko keamanan siber;
i. mengevaluasi akurasi dan validitas data yang digunakan oleh Bank untuk mengukur risiko keamanan siber;
j. menyusun dan menyampaikan laporan insiden siber, laporan penilaian maturitas penerapan manajemen risiko keamanan siber kepada Direksi dengan tembusan kepada Dewan Komisaris secara berkala; dan
k. melaksanakan kaji ulang secara berkala dengan frekuensi yang disesuaikan kebutuhan Bank untuk memastikan kecukupan kerangka manajemen risiko keamanan siber, keakuratan metodologi penilaian risiko keamanan siber, dan kecukupan sistem informasi manajemen risiko siber.

B.1.4. Budaya dan Kesadaran

41. Direksi harus mengembangkan budaya bahwa seluruh pegawai di semua level memiliki tanggung jawab penting dalam memastikan terciptanya keamanan siber. Budaya ini harus disampaikan melalui komunikasi yang jelas dan efektif serta mencakup informasi yang relevan tentang strategi keamanan siber kepada seluruh pegawai.

42. Direksi harus 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,* serta diseminasi kebijakan dan prosedur keamanan siber. Program kesadaran dimaksud harus dikaji secara berkala untuk memastikan substansi program sesuai dengan isu dan risiko siber yang relevan dan sedang berkembang.
43. Bank harus mengkinikan program kesadaran keamanan siber untuk menyesuaikan dengan teknologi terbaru, standar, dan persyaratan bisnis lainnya serta mengatasi adanya ancaman.
44. Bank harus memastikan bahwa seluruh pegawai mengetahui dan menerapkan kebijakan keamanan siber secara efektif, termasuk pula pegawai baru, serta menunjukkan perilaku dan keahlian yang diperlukan dalam menerapkan pemahaman keamanan siber sehingga memberikan kontribusi terhadap efektivitas sistem manajemen keamanan siber. 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.

B.1.5. Kapasitas Sumber Daya Manusia

45. Bank harus mengembangkan dan mengimplementasikan program berkelanjutan untuk peningkatan kapasitas terkait keamanan siber untuk 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.
46. Program peningkatan kapasitas dimaksud paling sedikit harus mencakup:

a. identifikasi ancaman siber saat ini termasuk berbagai bentuk serangan *social engineering,* antara lain *phising, scam phone,* dan *impersonation call*;
b. taktik serangan siber;
c. pengamanan termasuk penggunaan *secure authentication* dan cara mengidentifikasi dan melindungi, menyimpan, mengirimkan, mengarsipkan, dan memusnahkan informasi sensitif dengan benar;
d. sebab-sebab kebocoran data secara tidak sengaja, seperti kehilangan perangkat seluler karyawan atau ketidaksengajaan mengirim email ke orang yang salah,
e. perlindungan data, pembatasan penggunaan, dan dokumentasi proses penanganan data sensitif stakeholder,
f. kewajiban menjaga data privasi dan hukum pengungkapan data yang salah,
g. pembuatan *secure code* yang baik dalam pengembangan *software*/aplikasi, dan
h. praktik respon insiden yang tepat.

Frekuensi dan substansi pelatihan harus disesuaikan dengan peran dan tanggung jawab masing-masing pegawai.

47. Bank harus melakukan analisis kesenjangan (*gap analysis*) untuk memahami pengetahuan dan kemampuan yang tidak dimiliki pegawai terkait keamanan siber dan mengunakan informasi tersebut untuk membuat rencana aksi peningkatan kapasitas pegawai melalui antara lain pendidikan dan pelatihan terkait keamanan siber paling sedikit 2 (dua) kali dalam setahun. Dalam melakukan peningkatan kapasitas pegawai Bank dapat mengacu pada ketentuan teknis peningkatan kapasitas sumber daya manusia yang diterbitkan oleh badan yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

B.2. Kerangka Manajemen Risiko Keamanan Siber

48. Kerangka manajemen risiko keamanan siber paling sedikit mencakup (i) penetapan tingkat risiko yang akan diambil dan toleransi risiko terkait keamanan siber; (ii) penetapan strategi manajemen risiko keamanan siber; dan (iii) kebijakan, prosedur, dan penetapan limit.

B.2.1. Penetapan Tingkat Risiko Yang Akan Diambil dan Toleransi Risiko Terkait Keamanan Siber

49. Direksi bertanggung jawab untuk menetapkan tingkat risiko yang diambil terkait dengan keamanan siber Bank. Tingkat risiko yang akan diambil merupakan tingkat yang bersedia diambil oleh Bank dalam rangka mencapai sasaran tingkat maturitas penerapan manajemen risiko keamanan siber Bank. Tingkat risiko yang akan diambil tercermin dalam strategi dan sasaran manajemen risiko keamanan siber Bank secara keseluruhan.
50. Direksi bertanggung jawab untuk menetapkan toleransi risiko terkait dengan keamanan siber Bank. Toleransi risiko terkait dengan kemampuan Bank untuk menerima kejadian risiko siber dan dampaknya. Toleransi risiko merupakan penjabaran lebih lanjut dari tingkat risiko yang akan diambil terkait keamanan siber.
51. 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*).

B.2.2. Strategi Manajemen Risiko Keamanan Siber

52. Bank harus merumuskan strategi manajemen risiko keamanan siber yang sepadan dengan kerentanan dan tingkat eksposur Bank terhadap ancaman siber serta sejalan baik dengan tingkat risiko yang akan diambil dan toleransi risiko terkait keamanan siber maupun strategi bisnis secara keseluruhan.

53. Strategi manajemen risiko keamanan siber disusun untuk memastikan bahwa eksposur risiko keamanan siber Bank dikelola secara terkendali sesuai dengan kebijakan dan prosedur internal Bank serta peraturan perundang-undangan dan ketentuan lain.
54. Selain mempertimbangkan kebutuhan terhadap keamanan siber bank saat ini, strategi manajemen risiko keamanan siber harus berorientasi jangka menengah dan jangka panjang untuk memastikan kelangsungan usaha Bank.
55. Strategi Manajemen Risiko disusun dengan mempertimbangkan berbagai faktor termasuk namun tidak terbatas 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, dan kondisi keuangan Bank.
56. Bank harus memastikan bahwa seluruh peran dan tanggung jawab terkait keamanan siber didefinisikan dengan jelas dalam strategi manajemen risiko keamanan siber. Strategi manajemen risiko keamanan siber Bank paling sedikit harus mencakup uraian atas hal-hal sebagai berikut:
    a. Pemahaman institusional tentang risiko siber secara keseluruhan dan kaitannya dengan bisnis dan operasi lembaga keuangan, tingkat eksposur terhadap risiko siber, dan kondisi keamanan siber Bank saat ini;
    b. Identifikasi, klasifikasi, dan prioritisasi sistem kritis, informasi, aset, dan keterkaitan (*interconnectivity*) untuk memperoleh pemahaman yang lengkap dan akurat tentang profil risiko siber Bank;
    c. Identifikasi ancaman dan penanggulangan permasalahan keamanan siber, termasuk langkah-langkah yang diperlukan untuk menanggulangi risiko reputasi yang dapat merusak kepercayaan nasabah terhadap Bank;
    d. Kontrol keamanan untuk melindungi data, infrastruktur, dan aset Bank terhadap ancaman siber yang berkembang;
    e. Deteksi insiden keamanan siber secara tepat waktu melalui pengawasan dan pemantauan secara berkala; dan

f. 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.

57. Direksi harus mengkomunikasikan strategi manajemen risiko keamanan siber secara efektif kepada seluruh satuan kerja dan pegawai agar dipahami secara jelas.
58. Direksi harus melakukan kaji ulang strategi manajemen risiko keamanan siber secara berkala untuk menentukan apakah perlu dilakukan perubahan terhadap strategi manajemen risiko tersebut.

B.2.3. Kebijakan, Prosedur, dan Limit

59. Direksi harus menetapkan kebijakan, prosedur, dan penetapan limit yang dituangkan secara tertulis dalam menerapkan manajemen risiko keamanan siber.
60. Kebijakan, prosedur, dan penetapan limit tersebut harus harus sejalan dengan visi, misi, dan strategi bisnis Bank.
61. Kebijakan dan prosedur harus didesain dan diimplementasikan 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.
62. Kebijakan manajemen risiko keamanan siber termasuk strategi dan tujuan manajemen risiko siber harus diinternalisasikan ke dalam proses bisnis seluruh lini bisnis dan aktivitas pendukung, termasuk kebijakan yang bersifat spesifik sesuai dengan kebutuhan lini bisnis dan aktivitas pendukung Bank.
63. Kebijakan manajamen risiko keamanan siber secara umum harus memenuhi antara lain:
    a. memuat bagaimana Bank menetapkan toleransi risiko keamanan siber dan tata cara Bank mengidentifikasi, mengurangi, dan mengelola risiko keamanan siber untuk mencapai keamanan siber Bank;

b. memuat pokok-pokok prinsip manajemen keamanan siber ini, antara lain terkait *governance, strategy, identification, protection, vigilance, resilience,* dan *internal control system;*

c. memuat rencana kelangsungan usaha (*business continuity plan* atau *business continuity management*) atas kemungkinan kondisi eksternal dan internal terburuk dari serangan keamanan siber, antara lain melalui pelaksanaan *business impact analysis* secara berkala, sehingga kelangsungan usaha Bank dapat dipertahankan termasuk dengan menyertakan prosedur ketahanan dan kelangsungan usaha atas serangan keamanan siber dalam rencana pemulihan bencana (*disaster recovery plan*) dan rencana kontinjensi (*contingency plan*);

d. disusun dengan menggunakan standar dan pedoman internasional dan nasional sebagai *benchmark*; dan

e. konsisten dengan kerangka manajemen risiko Bank secara keseluruhan.

64. Bank juga harus membuat kebijakan manajemen risiko keamanan siber lebih spefisik yang memuat antara lain:

a. Perlindungan data,

b. Kepatuhan sumber daya manusia terhadap kebijakan manajemen risiko 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 melakukan ancaman keamanan siber;

e. Metode manajemen data termasuk namun tidak terbatas pada perlindungan data, transfer data, dan penghapusan data;
f. Metode pengendalian kriptografi;
g. Kepatuhan terhadap peraturan mengenai hak kekayaan intelektual; dan
h. Metode verifikasi seluruh perangkat keras dan perangkat lunak yang diperoleh dari luar Bank termasuk namun tidak terbatas melakukan analisis statis dan/atau dinamis untuk memverifikasi bahwa praktik *secure coding* telah diterapkan dengan baik.

65. Bank harus memiliki prosedur yang merupakan turunan dari kebijakan manajemen risiko siber, dapat berupa kontrol 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.
66. Bank harus memiliki proses, prosedur, dan kebijakan keamanan informasi (mengatur tujuan, cakupan, fungsi, tanggung jawab, komitmen manajemen, dan koordinasi antar entitas organisasi) yang dikelola dan digunakan untuk mengatur pelindungan sistem informasi dan aset.
67. Bank harus memiliki limit risiko 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.
68. Dalam rangka pengendalian risiko keamanan siber, limit digunakan sebagai ambang batas untuk menentukan tingkat intensitas mitigasi risiko keamanan siber yang akan dilaksanakan manajemen.
69. Kebijakan, prosedur, dan penetapan limit dalam penerapan manajemen risiko keamanan siber harus didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.

70. Direksi harus melakukan kaji ulang kebijakan, prosedur, dan penetapan limit dalam penerapan manajemen risiko keamanan siber secara berkala untuk menyesuaikan dengan kondisi terkini.

71. Bank harus memiliki program untuk meningkatkan kesadaran karyawan dan nasabah terkait kerentanan siber yang berkembang saat ini, misalnya *social engineering* dan cara melakukan pencegahannya, serta menetapkan proses penerimaan dan penanganan laporan kerentanan, termasuk penyediaan sarana bagi nasabah untuk membuat laporan kepada Bank, serta melakukan evaluasi efektivitas program dimaksud.

B.3. Proses Identifikasi, Perlindungan, Ketanggapan, dan Ketahanan serta Sistem Informasi Manajemen Risiko Keamanan Siber

B.3.1. Identifikasi

72. Proses identifikasi paling sedikit mencakup manajemen aset serta asesmen ancaman dan kerentanan.

73. Dalam melaksanakan proses manajemen aset, Bank harus memperhatikan hal-hal sebagai berikut:
    a. melakukan analisis, penilaian, dan klasifikasi atas aset, infrastruktur, dan informasi berdasarkan tingkat kritikalitas dan sensitivitasnya terhadap bank;
    b. mencatat (memiliki *record*), dan memperbaharui secara teratur seluruh fungsi kritis Bank, termasuk aset informasi, peran personel kunci, dan proses yang mendukung fungsi tersebut;
    c. melakukan inventarisasi aset TI dan aplikasi, berikut dengan data yang dimuat di dalamnya, dengan prioritisasi (berdasarkan klasifikasi kritikalitas dan sentivitas) serta memastikan aset TI dan aplikasi telah sesuai dengan kebutuhan Bank;

d. memastikan Bank telah memiliki *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak; dan
e. menyusun dan memelihara inventaris jaringan secara berkala, termasuk IP, perangkat, server, dan tautan jaringan eksternal yang mendukung fungsi penting Bank terkait dengan kerentanannya terhadap ancaman siber.

74. Dalam melaksanakan proses asesmen terhadap ancaman dan kerentanan, Bank harus memperhatikan hal-hal sebagai berikut:
    a. melakukan pemantauan seluruh sistem secara berkala untuk mengidentifikasi kelemahan dan kerentanan (*vulneralibility assessment*) dan memastikan risiko yang timbul dari celah tersebut dapat ditangani dengan memadai dan tepat waktu;
    b. menetapkan frekuensi pelaksanaan *vulnerability assessment* dengan menyesuaikan pada tingkat kritikalitas sistem dan risiko yang dihadapi;
    c. melakukan analisis atas ancaman dan kerentanan serta melakukan klasifikasi ancaman dan kerentanan berdasarkan potensi dampak yang dapat ditimbulkan;
    d. melakukan pemantauan terhadap perkembangan ancaman siber yang terkini (*emerging cyber threat*), baik dari sisi teknologi, taktik dan teknik serangan, serta prosedur atau pola serangan;
    e. menyusun dan memelihara inventaris risiko (*risk repository*) sesuai dengan hasil pemantauan yang diperbaharui secara berkala, terutama untuk aplikasi yang memproses data nasabah atau *stakeholders* lainnya; dan
    f. melakukan penilaian ancaman dan kerentanan sebelum menerapkan dan/atau memperbaharui teknologi, produk, layanan, dan/atau koneksi baru dan melakukan pembaharuan penilaian jika Bank mengidentikasi informasi baru yang dapat mempengaruhi risiko keamanan siber (misalnya ancaman dan/atau kerentanan baru, perubahan perangkat keras dan/atau lunak, perubahan konfigurasi, atau hasil tes yang berpotensi merugikan).

B.3.2. Perlindungan

75. Bank harus menerapkan seperangkat pengendalian keamanan (*security control*) yang komprehensif berdasarkan identifikasi fungsi kritis, peran kunci, proses, aset informasi, penyedia layanan pihak ketiga, dan interkoneksi, sesuai penilaian risiko dalam fase identifikasi. Pengendalian keamanan tersebut dapat mencakup:
    a. keberlangsungan dan ketersediaan sistem informasi;
    b. integritas informasi yang disimpan dalam sistem informasi;
    c. perlindungan integritas, kerahasiaan, dan ketersediaan data dan informasi; dan
    d. kesesuaian dengan hukum, peraturan, dan standar yang berlaku.
76. Bank harus melakukan pemeliharaan dan perbaikan terhadap pengendalian komponen sistem informasi sesuai dengan kebijakan dan prosedur yang berlaku.
77. Bank harus menerapkan teknologi keamanan yang dikelola dengan baik untuk mencapai keamanan dan ketahanan sistem serta data dan informasi sesuai dengan kebijakan dan prosedur yang berlaku.
78. Bank harus secara teratur memperbarui kontrol keamanannya untuk memastikan pendekatan yang diadopsi tetap sepadan dengan fungsi kritis entitas dan lanskap ancaman siber.
79. Bank menerapkan manajemen keamanan data dan informasi (baik elektronik dan *hard copy*) dan memastikan bahwa informasi dan dokumen dikelola sesuai dengan strategi risiko organisasi untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi. Manajemen keamanan data tersebut paling sedikit mencakup:
    a. Perlindungan *data-at-rest, data-at-endpoint,* dan *data-in-transit,* antara lain dengan melakukan enkripsi data dan/atau informasi pada saat disimpan maupun pada saat dikirim;

b. Pengelolaan aset (informasi dan data) yang memadai (aset yang dipindahkan, didisposisi, atau tidak dipakai);
c. Perlindungan terhadap ketersediaan data dan informasi, meliputi kepemilikan data, metadata periode retensi, dan penggunaannya terutama sehubungan dengan data sensitif, termasuk data *stakeholder* Bank;
d. Mekanisme pengecekan integritas terhadap verifikasi perangkat lunak, perangkat keras, serta integritas data dan informasi;
e. Pemisahan antara lingkungan pengembangan dan pengujian dari lingkungan produksi;
f. Penggunaan mekanisme pemeriksaan integritas data dalam verikasi perangkat keras;
g. Proses *backup data* yang dilakukan sesuai dengan kebutuhan bisnis dari hasil *Business Impact Analysis* dan penyimpanan *data backup* yang dilindungi baik secara fisik maupun non-fisik;
h. Dokumentasi dan proses penghimpunan data dan informasi dari pihak ketiga, antara lain vendor, departemen pemerintah terkait, lembaga pelatihan, dll, dalam hal pelaporan insiden keamanan seperti dalam rangka penegakan hukum, dll, termasuk monitoring dan pelaporan berkala, serta retensi data sensitif sesuai kebutuhan bisnis; dan
i. Penerapan metode otomatis untuk sinkronisasi *critical system clocks* seperti *Network Time Protocol*.

80. Bank menerapkan manajemen perlindungan terhadap infrastruktur (antara lain jaringan, aplikasi, dan perangkat) dengan memperhatikan hal-hal sebagai berikut:
a. memiliki perangkat perlindungan jaringan perimeter (misalnya *border router* dan *firewall*) yang memadai dan diverifikasi secara berkala, termasuk *implicit* atau *explicit deny rule*;

b. memiliki *Intrusion Prevention System* (IPS) atau *Intrusion Detection System* (IDS) untuk mendeteksi dan menghalangi percobaan serangan atau gangguan;
c. implementasi pembatasan terhadap *inbound* dan *outbound network traffic* dalam jaringan untuk mencegah *malware*;
d. menggunakan *next generation endpoint protection* untuk membatasi aplikasi yang diunduh, diinstal, dan diaplikasikan;
e. melakukan pemantauan terhadap *port* jaringan secara berkala;
f. menggunakan autentifikasi terpusat untuk seluruh perangkat jaringan;
g. adanya proses enkripsi untuk autentifikasi dan transmisi data melalui jaringan nirkabel dan perangkat *mobile* baik milik Bank maupun pengguna, serta media penyimpanan eksternal;
h. memiliki perangkat untuk mencegah tindakan tidak terautorisasi pada perangkat, infrastuktur jaringan, dan komponen sistem yang dikelola oleh Bank;
i. memiliki perangkat keamanan jaringan, misalnya *Domain Name System* (DNS) *filtering service* atau DNS *Security Extensions;*
j. memiliki sistem pengecekan otomatis terhadap *spam/phising/malware* pada *email* termasuk yang ada di dalam *cloud;*
k. menggunakan pembatasan penggunaan *scripting tools* (misalnya *Microsoft PowerShell* dan *Phyton*);
l. 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,* dan lain sebagainya, serta memastikan *update support* tersebut segera dilakukan dalam hal terdapat *security patches;*
m. menggunakan *add-on* dan *plugin* aplikasi sesuai dengan ketentuan organisasi;

n. memastikan kecukupan proses formal pengelolaan konfigurasi router, switch dan firewall, meliputi perubahan dan pengujian semua perubahan konfigurasi *router, switch*, dan *firewall*; dokumentasi konfigurasi dan reviu berkala atas konfigurasi *router* dan *switch* minimal setiap 6 bulan; sinkronisasi *switch* dan *router startup configs* dengan *running configs*; kebijakan akun *default* konfigurasi, serta *backup* atas konfirugasi perangkat tersebut;

o. mengidentifikasi dan membatasi akses perangkat yang tidak diizinkan;

p. membatasi penggunaan aset untuk kepentingan pribadi dan penggunaan aset pihak ketiga pada jaringan Bank;

q. menetapkan hak akses administrator pada perangkat Bank untuk pegawai;

r. menonaktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh Bank (port usb, dvd, akses smartphone, dll); dan

s. menerapkan *whitelist* aplikasi untuk memastikan bahwa hanya *authorized software library* dan *signed script* yang dapat dijalankan oleh sistem.

81. Bank menerapkan manajemen perlindungan terhadap akses dan pengguna dengan memperhatikan hal-hal sebagai berikut:

a. implementasi identifikasi dan autentifikasi pengelolaan akses terhadap seluruh sistem, aplikasi, dan *hardware;*

b. terdapat kendali terhadap akses pengguna, termasuk *password complexity,* pembatasan percobaan dan penggunaan kembali *passwords* serta permintaan *password* setelah perangkat tidak aktif untuk beberapa saat;

c. menerapkan pengamanan *endpoint* antara lain dengan menggunakan *web URL filtering, device control,* dan *aplikasi control* pada seluruh perangkat *endpoint* pengguna termasuk *endpoint* yang terhubung ke VPN;

d. menggunakan verifikasi *on time password* (OTP) untuk transaksi yang berisiko tinggi;

e. menerapkan *IP reputation* untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi;
f. memastikan batasan akses pada *database,* misalnya menerapkan akses *read-only* bagi pengguna selain admin *database;*
g. menggunakan *Multi-Factor Authentication* (MFA) untuk akses data sensitif atau akses terhadap seluruh jaringan apabila diperlukan;
h. menonaktifkan komunikasi antar *work station* untuk mencegah terjadinya serangan siber dan *disabled peer to peer* pada *wireless client* di perangkat *endpoint;*
i. memastikan karyawan menggunakan fitur *wireless* hanya untuk kepentingan Bank;
j. menonaktifkan fitur *auto-run content* terhadap perangkat yang terhubung ke sistem atau perangkat di Bank; dan
k. menerapkan metode autentifikasi melalui saluran terenkrepsi, baik untuk *login* terhadap jaringan maupun aplikasi.

82. Dalam hal Bank menggunakan *cloud* maka Bank harus memperhatikan hal-hal sebagai berikut:
a. memastikan telah terdapat pengendalian yang memadai untuk *logical access* ke sistem bank;
b. menerapkan kebijakan klasifikasi kritikaslitas dan sensitivitas terhadap data dan informasi yang disimpan pada *cloud;*
c. memastikan pengamanan yang menjadi tanggung jawab bank (*security in the cloud*) telah dikonfigurasikan sesuai standar dan *best practices;*
d. memastikan kapabilitas SDM bank untuk dapat mengkofigurasikan sistem dan menerapkan kontrol pengamanan di *cloud;*`
e. menggunakan *authorized cloud storage;*
f. memastikan autoritasi *traffic* pada layanan *cloud* hanya untuk kebutuhan bisnis dan operasional Bank;

g. membatasi akses *traffic cloud* hanya untuk alamat IP yang dikenal oleh Bank;

h. memastikan penyedia *cloud* telah menerapkan *Multi-Factor Authentication;*

i. memastikan penyedia *cloud* memiliki *Data Center Redundancy* yang terpisah secara geografis dan memiliki *Recovery Point* dan *Recovery Time Objective* yang terdokumentasi; dan

j. Memastikan penerapan *single-sign on* serta aksesnya melalui SSL VPN *tunnel*.

83. Bank harus memastikan penerapan *secure coding* dalam pengembangan sistem dan aplikasi untuk memastikan integritas sistem dan aplikasi dengan memperhatikan hal-hal sebagai berikut:

a. memastikan *developer* sistem dan aplikasi mengikuti praktik *secure programme coding* sebagai bagian dari *system development life cycle;*

b. melakukan *review* dan pengujian secara berkala terhadap keamanan *software* yang dikembangkan oleh internal Bank maupun pihak ketiga;

c. melakukan peninjauan *source code* untuk mendeteksi kerentanan terhadap perangkat lunak, terutama sebelum masuk ke tahap *production;* dan

d. memastikan kesesuaian praktik dengan bahasa pemrogaman dan *development environment* yang digunakan.

84. Bank harus memastikan program pengelolaan *patch* berjalan dengan baik memastikan keandalan dan kemutakhiran seluruh komponen perangkat lunak dan infrastruktur TI Bank dengan memperhatikan hal-hal sebagai berikut:

a. memastikan proses *patch* dilakukan dengan tepat waktu sesuai dengan tingkat kritikalitas berdasarkan prioritiasi kebutuhan *patch* pada jaringan dan infrastruktur;

b. melakukan kaji ulang atas program pengelolaan *patch,* termasuk *scanning* ulang untuk memastikan bahwa kerentanan telah ditutup dengan baik; dan

c. mendokumentasikan proses dan prosedur pengelolaan *patch.*

B.3.3. Ketanggapan

85. Bank harus memiliki dokumentasi kinerja dasar atas fungsi kritis Bank dan sistem pendukung, sehingga setiap penyimpangan dapat dideteksi secara tepat waktu dan aktivitas dan kejadian anomali dapat ditandai untuk diselidiki, proses tersebut dapat memperhatikan hal-hal sebagai berikut:

a. memastikan bahwa Bank memiliki kemampuan yang tepat dalam hal SDM, proses, dan teknologi untuk mendeteksi penyimpangan dari kinerja dasar sistem;

b. melakukan analisis untuk memahami penyebab atas kejadian, target dan metode serangan atau kejadian, serta dampak yang dapat ditimbulkan atas suatu kejadian;

c. memiliki kriteria batasan yang dapat memicu peringatan/tanda ketika terdapat aktivitas atau kejadian anomali;

d. 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

e. melakukan sentralisasi dan pengkoordinasian proses keamanan siber dan teknologi dalam suatu *Security Operations Center* (SOC) atau yang sejenis.

86. Bank melakukan pemantauan atau deteksi berkelanjutan terhadap kerentanan untuk memastikan efektivitas upaya perlindungan yang telah diterapkan. Deteksi kerentanan dilakukan dengan memperhatikan hal-hal sebagai berikut:

a. pemantauan berkelanjutan terhadap lalu lintas jaringan, *log*, aktivitas personil dan pegawai, deteksi terhadap *malicious code,* deteksi terhadap

unauthorized encription and mobile code, deteksi *wireless access point* kepada LAN (*ethernet*), jasa yang disediakan oleh pihak eksternal Bank, pemantauan terhadap personil, koneksi, perangkat, dan perangkat lunak yang tidak sesuai kewenangan, akses dan perubahan pada data sensitif, serta akses fisik terhadap perangkat yang berada dalam ruangan *data center*;

b. mengimplementasikan sistem untuk pemantauan dan pencegahan kehilangan data sensitif termasuk *data* nasabah dan *stakeholders* (contohnya penggunaan *Data Loss Prevention*);

c. mengaktifkan DNS *query logging* dalam mendeteksi *hostname lookups* untuk mengetahui adanya *malicious domain;*

d. melakukan *independent testing* sesuai dengan penilaian risiko terhadap jaringan internal dan sistem yang terpapar jaringan eksternal;

e. melakukan analisis atas *security control gaps* berdasarkan hasil *independent testing* yang dilakukan secara berkala; dan

f. memiliki sumber terkait isu terkini keamanan siber (misalnya melalui *managed security service provider* atau penyedia produk keamanan siber, *multiple threar intilligence feeds,* dan *cyber threat intelligence unit*).

87. Bank harus melakukan pemantauan atas aktivitas mencurigakan dan melakukan pengelolaan dan pengujian proses dan prosedur deteksi untuk memastikan aktivitas anomali dapat dideteksi secara tepat waktu. Pemantauan aktivitas mencurigakan dilakukan dengan memperhatikan hal-hal sebagai berikut

a. mengimplementasikan *Security Information and Event Management* (SIEM) atau *Log Analytic Tools* untuk keperluan dokumentasi, korelasi, dan analisis *log*;

b. 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;

c. melakukan *backup* 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;
d. melakukan prioritisasi atas kejadian (*event*) dalam *log* berdasarkan tingkat keparahan/dampak, dan kategori keamanan;
e. melakukan deteksi atas akses yang tidak diautorisasi, kegagalan *login* pada perangkat jaringan, *server,* dan aplikasi, serta anomali pada jaringan;
f. memiliki sistem notifikasi atas transaksi nasabah yang dapat tergolong sebagai aktivitas mencurigakan;
g. menindaklanjuti transaksi anomali dan memberikan notifikasi kepada nasabah atau pengguna layanan; dan
h. melakukan pemantauan dan analisis perilaku pegawai (pola penggunaan jaringan, perangkat, dan jam kerja) untuk mendeteksi potensi aktivitas mencurigakan.

88. Bank harus melakukan deteksi atas insiden siber dengan memperhatikan hal-hal sebagai berikut:
    a. memastikan mekanisme deteksi (*anti-virus and anti-malware alerts, log event alerts*) berjalan dengan baik untuk memberikan peringatan atas insiden atau serangan;
    b. memastikan bahwa *log* hasil deteksi terhubung dengan *event log servers* dan dapat digunakan untuk analisis;
    c. memiliki proses kolaborasi informasi kejadian siber dari berbagai sumber, seperi jaringan, aplikasi, atau *firewall;*
    d. memastikan bahwa kemampuan deteksi dan pemantauan dapat menyediakan informasi yang memadai untuk mendukung analisis atas kejadian dan insiden yang terjadi; dan

e. memastikan adanya *ticketing system* yang digunakan untuk melacak progres dari *event post-notification* serta mengkategorisasikan kejadian berdasarkan tingkat keparahan/priotitas/dampak, kategori keamanan, dan jenis log yang berkorelasi.

89. Bank harus melakukan analisis terhadap ancaman dan kerentanan siber untuk memastikan penanganan insiden secara tepat sehingga dapat mencegah terjadinya gangguan pada layanan dan/atau operasional Bank. Dalam melakukan analisis terhadap dan kerentanan siber, Bank memperhatikan hal-hal sebagai berikut:
    a. menggunakan informasi yang tersedia untuk meningkatkan sistem pengendalian intern dan manajemen risiko keamanan siber Bank;
    b. 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;
    c. memperoleh atau menyusun informasi mengenai ancaman siber yang antara lain terdiri atas *Indicator of Compromise* (IOC), artefak jaringan, *tools* yang digunakan, 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
    d. menggunakan *security metrics* untuk mengevaluasi efisiensi penerapan keamanan siber dan melakukan kaji ulang secara berkala.

B.3.4. Ketahanan

90. Bank harus memiliki rencana penanganan dan pemulihan saat insiden atau serangan siber terjadi untuk memastikan respon yang tepat waktu untuk mengembalikan layanan secepat mungkin dengan yang dampak minimal. Rencana penanganan dan pemulihan dimaksud paling sedikit harus mencakup dan memperhatikan hal-hal sebagai berikut:

a. Kategorisasi fungsi kritis sebagaimana proses identifikasi untuk menentukan prioritas pemulihan sistem dan layanan;
b. Pelaporan dan eskalasi di intern Bank, termasuk kepada senior manajemen dan Direksi, berdasarkan potensi dampak dari insiden siber;
c. Peran dan tanggung jawab yang jelas untuk seluruh pegawai yang terlibat dalam proses eskalasi, respon, dan pemulihan insiden siber;
d. Menguraikan alur komunikasi kepada pemangku kepentingan internal dan eksternal yang perlu dikomunikasikan tentang insiden siber dan praktik/teknik kerentanan siber yang berkembang saat ini yang dapat digunakan dalam peningkatan risiko fraud/penipuan, termasuk waktu pemberitahuan, dan cakupan informasi yang perlu dikomunikasikan. Tingkat keterlibatan pemangku kepentingan ditentukan oleh tingkat keparahan dan dampak insiden siber;
e. Bank mempertimbangkan berbagai skenario insiden siber dalam merumuskan rencana penanganan dan pemulihan serta melakukan analisis dampak atas insiden terhadap aktivitas Bank; dan
f. Rencana penanganan dan pemulihan Bank harus sesuai dengan *business continuity plan, disaster recovery plan, crisis management plan,* dan/atau kebijakan atau rencana Bank lainnya yang terkait.

91. Direksi perlu melakukan kaji ulang secara berkala terhadap rencana penanganan dan pemulihan insiden siber Bank.
92. Bank harus membentuk serta menetapkan peran serta tugas dan tanggung jawab *Cyber Incident Response Team* untuk memastikan penanganan dan pemulihan insiden siber dengan dampak minimal terhadap layanan dan opersional Bank. Dalam membentuk *Cyber Incident Response Team,* Bank dapat memperhatikan hal-hal sebagai berikut:
    a. memastikan bahwa pegawai yang terlibat dalam *Cyber Incident Response Team* memiliki kapasitas dan kemampuan terkait penanganan insiden siber, yaitu dengan melakukan latihan respon insiden secara rutin terkait

penujian saluran komunikasi, analisis insiden, pengambilan keputusan dan rekomendasi solusi, serta kemampuan teknis pelaporan insiden;

b. memastikan bahwa *Cyber Incident Response Team* dapat bekerja sama dengan unit kerja/fungsi terkait (spesialis keamanan teknis, unit bisnis, fungsi legal, SDM, dan tim komunikasi eksternal) dan dapat dengan cepat mengakses informasi yang diperlukan (misalnya dari penyedia jasa pihak ketiga atau informasi pendukung penting lainnya);

c. memastikan bahwa *Cyber Incident Response Team* memiliki sumber daya analisis insiden (misalnya daftar *host, packet snifer,* analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat *digital forensic,* dan sumber daya lain yang diperlukan); dan

d. memastikan bahwa *Cyber Incident Response Team* dapat bekerja sama secara efektif dengan fungsi *cyber threat intilligence,* dan *network operations* untuk menghadilkan penanganan insiden yang tepat dan proaktif terhadap potensi insiden di masa depan.

93. Bank harus melakukan analisis untuk memastikan langkah-langkah penanganan dan pemulihan insiden siber dijalankan dengan tepat, analisis dapat mencakup hal-hal sebagai berikut:

a. pemahaman terhadap dampak dari insiden siber, pelaksanaan penyelidikan forensik, dan kategorisasi insiden siber;

b. *root cause analysis* terhadap insiden siber untuk mencegah terulangnya kejadian serupa;

c. kaji ulang terhadap rekap laporan insiden siber untuk mempelajari kesesuaian prosedur insiden siber dengan standar dan prosedur yang telah ditetapkan; dan

d. mencatat setiap langkah yang dilakukan dalam rangka penanggulangan inisiden 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.

94. Bank harus menerapkan prosedur pemulihan dan upaya-upaya untuk mencegah suatu insiden menjadi berkembang dengan memitigasi efek dan menanggulangi insiden tersebut. Prosedur pemulihan dan upaya mitigasi dapat dilakukan dengan memperhatikan hal-hal sebagai berikut:
    a. memiliki rencana dan mengimplementasikan rencana *re-route* atau penggantian fungsi dan/atau jasa kritikal yang terdampak insiden siber;
    b. mengembangkan langkah penahanan (*containment*) dan mitigasi awal untuk mengembalikan operasional dengan gangguan layanan yang minimal sesuai dengan jenis insiden yang terjadi; dan
    c. memiliki proses untuk memastikan aset yang terdampak oleh insiden dan tidak dapat digunakan kembali untuk kegiatan operasional telah dihapus atau digantikan.
95. Bank harus menerapkan eskalasi dan pelaporan insiden yang paling sedikit mencakup hal-hal sebagai berikut:
    a. proses eskalasi internal kepada pihak yang berwenang untuk melakukan penanganan dan analisis insiden siber dengan standar jangka waktu tertentu;
    b. proses eskalasi internal untuk melaporkan pelaksanaan penanganan dan pemulihan insiden siber kepada Direksi dan Dewan Komisaris berdasarkan kriteria potensi dampak dan kritikalitas;
    c. proses klasifikasi insiden dan penyusunan *log* insiden siber;
    d. prosedur notifikasi kepada nasabah dan pihak lainnya yang terkait ketika terjadi insiden siber yang terkait pada akses tidak terautorisasi pada informasi/data nasabah dan/atau insiden siber yang dapat menyebabkan gangguan atau penurunan layanan Bank kepada nasabah;

e. prosedur komunikasi kepada pihak ketiga atas terjadinya insiden siber yang dapat berdampak pada operasional bisnisnya atau nasabah/kliennya; dan
f. prosedur komunikasi kepada media apabila diperlukan.

B.3.5. Sistem Informasi Manajemen Risiko Keamanan Siber

96. Sistem informasi manajemen risiko keamanan siber merupakan bagian dari sistem informasi manajemen yang harus dimiliki dan dikembangkan sesuai dengan kebutuhan Bank dalam rangka penerapan manajemen risiko keamanan siber yang efektif.
97. Sebagai bagian dari proses manajemen risiko, sistem informasi manajemen risiko keamanan siber digunakan untuk mendukung pelaksanaan proses identifikasi, perlindungan, ketanggapan, dan ketahanan risiko keamanan siber, serta pelaporan tingkat kematangan manajemen risiko keamanan siber yang lengkap, akurat, kini, dan utuh.
98. Sistem informasi manajemen risiko keamanan siber harus dapat memastikan:
    a. 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 keamanan siber untuk menilai, memantau, dan memigitas risiko keamanan siber yang dihadapi Bank dan/atau dalam rangka proses pengambilan keputusan oleh Direksi;
    b. efektivitas penerapan manajemen risiko keamanan siber mencakup kebijakan dan prosedur manajemen risiko keamanan siber serta penetapan limit risiko; dan
    c. tersedianya informasi tentang hasil atau realisasi penerapan manajemen risiko keamanan siber dibandingkan yang ditetapkan oleh Bank sesuai dengan kebijakan dan strategi penerapan manajemen risiko keamanan siber.

99. Sistem informasi manajemen risiko keamanan siber dan informasi yang dihasilkan harus disesuaikan dengan karakteristik dan kompleksitas kegiatan usaha Bank serta adaptif terhadap perubahan.
100. Kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko keamanan siber harus dikaji ulang secara berkala untuk memastikan bahwa cakupan tersebut telah memadai sesuai perkembangan tingkat kompleksitas kegiatan usaha Bank.
101. Sebagai bagian dari sistem informasi manajemen risiko keamanan siber, laporan tingkat kematangan manajemen risiko keamanan siber disusun secara berkala oleh Satuan Kerja Manajemen Risiko yang independen terhadap unit kerja yang melakukan kegiatan bisnis. Frekuensi penyampaian laporan kepada Direksi terkait dan komite manajemen risiko harus ditingkatkan sesuai kebutuhan terutama dalam hal kondisi pasar berubah dengan cepat.
102. Sistem informasi manajemen risiko keamanan siber harus mendukung pelaksanaan pelaporan kepada Otoritas Jasa Keuangan.
103. Dalam mengembangkan teknologi sistem informasi dan perangkat lunak baru, Bank harus memastikan bahwa penerapan sistem informasi dan teknologi baru tersebut tidak akan mengganggu kesinambungan sistem informasi Bank.
104. Dalam hal Bank memutuskan untuk menugaskan tenaga kerja alih daya (*outsourcing*) dalam pengembangan perangkat lunak dan penyempurnaan sistem, Bank harus memastikan bahwa keputusan penunjukan pihak ketiga tersebut dilakukan secara obyektif dan independen, dengan melalui proses *due diligence* yang menyeluruh sebelumnya. Dalam perjanjian atau kontrak alih daya harus dicantumkan klausul mengenai pemeliharaan dan pengkinian serta langkah antisipasi guna mencegah gangguan yang mungkin terjadi dalam pengoperasiannya.
105. Sebelum menerapkan sistem informasi manajemen yang baru, Bank harus melakukan pengujian untuk memastikan bahwa proses keluaran (*output*) yang dihasilkan telah melalui proses pengembangan, pengujian, dan penilaian

kembali secara efektif dan akurat, serta Bank harus memastikan bahwa data historus akuntansi dan manajemen dapat diakses oleh sistem atau perangkat lunak baru tersebut dengan baik.

106. Bank harus menatausahakan dan mengkinikan dokumentasi sistem yang memuat perangkat keras, perangkat lunak, basis data (*database*), parameter, tahapan proses, asumsi yang digunakan, sumber data, dan keluaran yang dihasilkan sehingga memudahkan pengendalian melekat dan pelaksanaan jejak audit.

B.4 Kecukupan Sistem Pengendalian Internal

107. Bank harus memiliki sistem pengendalian intern atas keamanan siber yang efektif. Pelaksanaan sistem pengendalian intern secara efektif dalam penerapan manajemen risiko keamanan siber Bank mengacu pada kebijakan dan prosedur yang telah ditetapkan. Penerapan prinsip pemisahan fungsi (*four eyes principle*) harus memadai dan dilaksanakan secara konsisten.
108. Sistem pengendalian inten 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.
109. Dalam menerapkan sistem pengendalian internal dimaksud, Bank secara umum harus memperhatikan antara lain:
    a. penerapan manajemen risiko keamanan siber telah mencapai hasil yang diharapkan;
    b. kesesuaian antara sistem pengendalian internal dengan tingkat risiko inheren dan penerapan manajemen risiko keamanan siber pada Bank;
    c. penetapan wewenang dan tanggung jawab untuk pemantauan kepatuhan kebijakan dan prosedur manajemen risiko keamanan siber serta penetapan limit risiko 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 keamanan siber;
e. struktur organisasi yang menggambarkan secara jelas tugas dan tanggung jawab masing-masing unit dan individu
f. pelaporan penerapan manajemen risiko 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 keamanan siber Bank;
i. pengujian dan kaji ulang yang memadai terhadap sistem informasi manajemen risiko 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.

110. Selain hal-hal umum diatas, Bank dalam melakukan pengendalian internal perlu juga memperhatikan hal-hal spesifik yang meliputi namun tidak terbatas pada:
    a. semua tanggung jawab keamanan siber dan keamanan informasi telah ditentukan dan dialokasikan serta terkoordinir dengan baik;
    b. kepatuhan atas kewajiban semua sumber daya manusia termasuk kontraktor untuk menerapkan keamanan siber dan keamanan informasi sesuai dengan kebijakan dan prosedur yang telah ditetapkan;

c. kecukupan persyaratan keamanan siber dan keamanan informasi terkait akses supplier terhadap aset Bank yang telah didokumentasikan dengan baik;
d. kecukupan pengujian terhadap keberadaan informasi yang dapat berguna bagi penyerang seperti network diagram, file konfigursai, laporan uji penetrasi, email, atau dokumen yang berisikan kata sandi atau informasi lain yang penting untuk sistem operasi;
e. kecukupan penetapan program untuk *vulnerability assessment* atau *penetrating testing* secara berkala kepada aplikasi *web*, aplikasi *client-based*, aplikasi *mobile*, *wireless*, *server*, dan perangkat jaringan;
f. kecukupan pembentukan 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 merespon 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. pengunaan 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 keamanan siber secara berkala;

o. pencegarahan atau pengurangan terhadap dampak/efek yang tidak diinginkan dari risiko 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 kemanan siber dalam seluruh fase perencanaan, pembangunan, dan Pengembangan semua proyek TI.

111. Bank harus melakukan kaji ulang dan evaluasi secara berkala terhadap penerapan manajemen risiko keamanan siber. Kaji ulang dan evaluasi tersebut

dilakukan oleh satuan kerja yang menangani fungsi manajemen risiko keamanan siber dan satuan kerja audit internal. Kaji ulang dan evaluasi tersebut dilakukan paling sedikit sekali setiap tahun.

112. Penerapan kaji ulang dan evaluasi yang dilakukan oleh satuan kerja fungsi manajemen risiko keamanan siber paling sedikit mencakup antara lain:
    a. Kesesuaian kerangka manajemen risiko keamanan siber, yang mencakup kebijakan, struktur organisasi, alokasi sumber daya, desain proses manajemen risiko, sistem informasi, pelaporan risiko operasional Bank, dan pelaksanaan manajemen risiko keamanan siber;
    b. metode, asumsi, dan variabel yang digunakan untuk mengukur risiko keamanan siber dan limit eksposur risiko keamanan siber;
    c. perbandingan antara hasil dari metode pengukuran risiko 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 keamanan siber yang ditetapkan dengan eksposur risiko keamanan siber yang sebenarnya atau aktual; dan
    f. penerapan manajemen risiko keamanan siber oleh satuan kerja bisnis atau satuan kerja pendukung.

113. Penerapan kaji ulang dan evaluasi yang dilakukan oleh satuan kerja internal audit secara umum mencakup antara lain:
    a. keandalan kerangka manajemen risiko keamanan siber, yang mencakup kebijakan, struktur organisasi, alokasi sumber daya, desain proses Manajemen Risiko, sistem informasi, dan pelaporan Risiko Bank; dan
    b. penerapan manajemen risiko keamanan siber oleh seluruh pegawai, termasuk kaji ulang terhadap pelaksanaan pemantauan oleh satuan kerja yang berfungsi menangani manajemen risiko keamanan siber.

114. Satuan kerja internal audit perlu pula melakukan evaluasi untuk hal-hal spesifik terkait manajemen risiko keamanan siber yang mencakup namun tidak terbatas pada antara lain:
    a. penerapan manajemen data termasuk perlindungan;
    b. pengunaan algoritma enkripsi dalam pengembangan perangkat lunak;
    c. penggunaan *tool vulnerability scanning* secara mandiri, yang mana hasil *vulnerability assessment* digunakan sebagai titik awal dalam melakukan *penetrating testing*;
    d. penggunaan akun khusus selain akun admin untuk melakukan *vulnerability testing*;
    e. pengendalian dan pemantauan atas akun pengguna atau sistem yang digunakan dalam melakukan *penetrating testing* untuk memastikan bahwa akun tersebut hanya digunakan untuk tujuan yang sah dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan;
    f. penerapan keamanan informasi
    g. pelaksanaan secara berkala *security risk assessment* dan *security risk treatment*;
    h. izin akses dari pengguna setidaknya setiap tiga bulan;
    i. dokumentasi/diagram yang menggambarkan semua aliran data di seluruh sistem dan jaringan termasuk pembaruannya; dan
    j. penerapan dan dokumentasi standar konfigurasi (*port, protocol, service*) untuk semua sistem, seperti operating system, software/aplikasi, dan lain lain.
115. Pihak yang melakukan kaji ulang dan evaluasi manajemen risiko keamanan siber harus independen dan memiliki kompetensi yang baik serta metode kaji ulang yang andal.
116. Hasil kaji ulang dan evaluasi tersebut disampaikan kepada Dewan Komisaris dan Direksi untuk diambil langkah perbaikan dan/atau penyempurnaan manajemen risiko keamanan siber.

117. Satuan kerja internal audit harus melakukan pemantauan terhadap perbaikan hasil temuan. Temuan yang belum ditindaklanjuti harus dilaporkan kepada Dewan Komisaris dan/atau Direksi untuk diambil langkah-langkah yang diperlukan.
118. Bank memiliki sistem rotasi rutin untuk menghindari potensi self-dealing, persekongkolan atau penyembunyian suatu dokumentasi atau aktivitas yang tidak wajar.

V. Penilaian Tingkat Maturitas Manajemen Risiko Keamanan Siber

119. Bank harus melakukan penilaian sendiri (*self assessment*) tingkat maturitas manajemen risiko keamanan siber secara berkala, penilaian tersebut dilakukan paling sedikit setiap semester untuk posisi akhir bulan Juni dan akhir bulan Desember. Penilaian sendiri (*self assessment*) tersebut dapat dikinikan sewaktu-waktu apabila diperlukan, terutama dalam hal terjadi kondisi yang mengganggu keamanan siber Bank secara signifikan.
120. Penilaian tingkat maturitas manajemen risiko keamanan siber dilakukan melalui tiga tahap. Pertama, penilaian risiko inheren dengan mengevlauasi parameter dan indikator risiko siber. Kedua, penilaian atas penerapan 4 (empat) aspek manajemen risko siber. Ketiga, penilaian keseluruhan atas tingkat maturitas manajemen risiko keamanan siber sebagai kesimpulan akhir.
121. Dalam melakukan penilaian atas risiko inheren, Bank harus memperhatikan berbagai parameter atau indikator kuantitatif maupun kualitatif, yang paling sedikit mencakup faktor-faktor sebagai berikut (i) teknologi, (ii) saluran distribusi, (iii) produk dan aktivitas, (iv) karakter organisasi, dan (v) *track record* ancaman siber.

122. Bank harus menetapkan tingkat risiko inheren keamanan siber. Penetapan tingkat risiko inheren dikategorikan ke dalam Peringkat 1 (Low), Peringkat 2 (Low to Moderate), Peringkat 3 (Moderate), Peringkat 4 (Moderate to High), dan Peringkat 5 (High).
123. Dalam melakukan analisis peringkat risiko siber inheren, Bank dapat menggunakan matriks definisi tingkat risko siber inheren sebagaimana terdapat pada Lampiran B Matriks Tingkat Risiko Keamanan Siber Inheren. Bank dapat memilih tingkat risiko inheren yang paling tepat untuk setiap aktivitas, layanan, atau produk dalam setiap kategori.
124. Dalam melakukan penilaian atas penerapan manajemen risiko keamanan siber, Bank harus memperhatikan 4 (empat) aspek (i) tata kelola, (ii) kerangka manajemen risiko, (iii) perlindungan, ketanggapan, ketahanan, dan (iv) sistem pengendalian internal. Bank perlu melakukan analisis secara komprehensif dengan memperhatikan keterkaitan antara satu aspek dengan aspek lainnya, serta memastikan kecukupan penerapannya antara lain dengan penilaian terhadap pengujian ketahanan keamanan siber sebagaimana Bab V antara lain mencakup *penetration testing* dan pengujian keamanan siber berbasis skenario.
125. Bank harus menetapkan tingkat penerapan manajemen risiko keamanan siber. Penetapan tingkat penerapan manajemen risiko keamanan siber dikategorikan ke dalam Peringkat 1 (Strong), Peringkat 2 (Satisfactory), Peringkat 3 (Fair), Peringkat 4 (*Marginal*), dan Peringkat 5 (*Unsatisfactory*).
126. Dalam melakukan analisis tingkat penerapan manajemen risiko keamanan siber, Bank dapat menggunakan matriks definisi tingkat penerapan manajemen risiko keamanan siber sebagaimana terdapat pada Lampiran C Matriks Tingkat Kualitas Penerapan Manajemen Risiko Keamanan Siber.
127. Berdasarkan hasil penilaian risiko inheren dan penerapan manajemen risiko keamanan siber, Bank harus menetapkan tingkat maturitas manajemen risiko keamanan siber. Penetapan tingkat maturitas manajemen risiko keamanan

siber dikategorikan ke dalam peringkat Peringkat 1 (*Advanced*), Peringkat 2 (*Managed*), Peringkat 3 (*Intermediate*), Peringkat 4 (*Evolving*), dan Peringkat 5 (*Baseline*).

128. Dalam melakukan analisis tingkat maturitas manajemen risiko keamanan siber, Bank dapat menggunakan matriks definisi tingkat maturitas manajemen risiko keamanan siber sebagaimana terdapat pada Lampiran D Matriks Tingkat Maturitas Manajemen Risiko Keamanan Siber.
129. Dalam hal berdasarkan hasil identifikasi dan penilaian Otoritas Jasa Keuangan ditemukan permasalahan atau pelanggaran yang secara signifikan mempengaruhi atau akan mempengaruhi keamanan siber Bank, Otoritas Jasa Keuangan berwenang untuk menurunkan peringkat risiko inheren, peringkat tingkat penerapan manajemen risiko keamanan siber, dan/atau peringkat tingkat maturitas manajemen risiko keamanan siber.

VI. Pengujian Ketahanan Keamanan Siber

130. Bank harus melakukan pengujian penetrasi (*penetration test*) yang mencakup *planning, discovery, attacks,* dan *reporting* untuk mendapatkan evaluasi mendalam tentang pertahanan keamanan sibernya. *Penetration test* ini perlu dilakukan secara berkala terhadap *software, hardware,* dan *application.* Selain itu *penetration test* juga perlu dilakukan sebelum Bank mengimplementasikan sistem atau aplikasi yang bersifat *online* atau dapat diakses melalui internet. Kombinasi antara *blue team and red team testing*[11] dapat dilakukan untuk

[11] *Blue team and red team testing* adalah teknik pengujian keamanan siber dengan menggunakan kombinasi antara dua tim keamanan siber, yaitu *red team* yang menguji ketahanan siber dengan mensimulasikan taktik, teknik, dan prosedur pelaku ancaman siber di dunia nyata dan *blue team* yang terdiri atas tim respon insiden yang bertugas terhadap pertahanan siber bank untuk mengidentikasi dan merespon insiden atau serangan dari *red team.* Pengujian ini didasarkan pada *threat intelligence* tertentu dan fokus pada kemampuan SDM, proses, dan teknologi (*people, process, and technology* entitas), dengan pengetahuan awal yang minimal. (FSB *Cyber Lexicon,* NIST *Computer Security Resource Center*)

layanan Bank yang bersifat *online*. Bank dapat mempertimbangkan untuk melakukan program *bug bounty* untuk menguji keamanan infrastruktur TI Bank dan melengkapi *penetration test*, yaitu dengan menggunakan *ethical hacker* untuk melakukan *penetration test* pada sistem Bank untuk menemukan kerentanan dalam sistem.

131. Frekuensi *penetration test* harus ditentukan berdasarkan beberapa faktor, seperti kekritisan sistem dan tingkat paparan sistem terhadap risiko siber. Untuk sistem yang dapat diakses secara langsung dari internet, Bank diharapkan dapat melakukan *peneration test* untuk melakukan validasi kecukupan kontrol keamanan paling sedikit satu kali dalam setahun atau setiap kali sistem mengalami perubahan atau pembaruan besar.
132. Selain *penetration test*, Bank harus melakukan pengujian keamanan siber berbasis skenario secara rutin untuk melakukan validasi atas respon dan pemulihan Bank, serta rencana komunikasi Bank dalam menghadapi ancaman siber. Dalam melakukan pengujian, 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 deteksi, respons, dan pemulihan ancaman siber. Simulasi ini harus dilakukan dengan terkendali di bawah pengawasan ketat untuk memastikan kegiatan yang dilakukan oleh *red team* tidak mengganggu sistem Bank. Untuk melakukan simulasi serangan yang realistis, skenario ancaman harus dirancang dan didasarkan pada ancaman siber yang menantang namun tetap mungkin terjadi. Bank juga dapat merancang skenario latihan melalui *threat hunting* yang menyeluruh, yaitu secara proaktif memburu aktivitas berbahaya, mencurigakan, atau berisiko yang lolos dari deteksi pada jaringan, titik akhir, dan kumpulan data, antara lain dengan menggunakan *threat intelligence* yang relevan dengan lingkungan TI mereka untuk mengidentifikasi pelaku ancaman yang dapat menimbulkan ancaman bagi Bank, dan mengidentifikasi taktik, teknik, dan prosedur yang dapat

digunakan dalam serangan tersebut. Bank juga dapat melaksanakan pengujian kesadaran keamanan siber (*cybersecurity awareness test*) terhadap sumber daya manusia dan nasabah bank dalam rangka pengendalian ancaman *social engineering*.

133. Hasil pengujian ketahanan keamanan siber perlu dilakukan kaji ulang dan disampaikan kepada Direksi sebagai landasan untuk perbaikan tata kelola, kebijakan dan prosedur, pengendalian internal, peningkatan kapasitas, dan kesadaran Bank terhadap keamanan siber.

VII. Pelaporan

134. Bank harus menyampaikan laporan terkait penerapan manajemen risiko keamanan siber kepada OJK secara berkala. Laporan tersebut mencakup (i) laporan hasil penilaian sendiri (*self assessment*) tingkat kematangan manajemen risiko keamanan siber, (ii) laporan insiden siber, dan (iii) laporan hasil pengujian pertahanan keamanan siber.
135. Bank harus menyampaikan laporan hasil penilaian sendiri (*self assessment*) tingkat kematangan manajemen risiko keamanan siber secara semesteran untuk posisi Juni dan Desember. Laporan tersebut berisikan penjelasan secara singkat mengenai hasil evaluasi dan tindak lanjut penerapan keamanan siber Bank, yang antara lain dapat mencakup kondisi risiko siber saat ini yang dihadapi Bank, kesenjangan *(gap*) dalam program keamanan siber Bank dan langkah-langkah yang dapat dilakukan untuk menutup kesenjangan dan mengelola risiko siber, kesadaran Bank terhadap perkembangan ancaman siber (*emerging cyber threat*) yang berpotensi mengganggu operasional Bank, kesesuaian strategi keamanan siber Bank dengan strategi bisnis dan kerakteristik Bank, hasil pengujian ketahanan siber secara berkelanjutan, dan pendelegasan tugas dan wewenang fungsi keamanan siber Bank. Laporan tersebut dapat dijadikan satu dengan laporan penilaian tingkat kesehatan

Bank. Dalam hal terjadi pengkinian penilaian tingkat kematangan manajemen risiko keamanan siber yang dilakukan sewaktu-waktu, Bank harus menyampaikan laporan kepada OJK paling lambat 10 (sepuluh) hari kerja setelah dilakukannya pengkinian penilaian.

136. Bank harus menyampaikan laporan insiden siber kepada OJK. Laporan insiden siber merupakan bagian dari proses eskalasi dan komunikasi yang terdiri atas notifikasi insiden awal dan laporan insiden. Pelaporan keamanan siber Bank juga perlu disesuaikan dengan mekanisme pelaporan insiden siber di lingkup nasional sebagaimana dikoordinasikan oleh badan yang menyelenggarakan tugas pemerintahan di bidang keamanan siber. Laporan insiden siber disampaikan dengan ketentuan sebagai berikut:
    a. Notifikasi insiden awal perlu disampaikan oleh Bank secepatnya kepada pengawas paling lambat 1x24 jam setelah insiden diketahui melalui *e-mail* atau media komunikasi lain. Cakupan dari notifikasi insiden antara lain detail insiden secara singkat dan penilaian dampak awal. Dalam hal terdapat perubahan kondisi atau atas permintaan dari pengawas, Bank dapat menyampaikan pengkinian informasi atas notifikasi insiden.
    b. Laporan insiden siber lengkap disampaikan oleh Bank secara bulanan yang mencakup kronologi insiden secara lengkap (langkah eskalasi, komunikasi, dan keterlibatan *stakeholders*), analisis *root cause* (faktor penyebab, tindak lanjut penyelesaian, dan langkah perbaikan), dan asesmen final (kesimpulan atas penyebab dan dampak insiden, serta *corrective action* Bank).
137. Bank harus menyampaikan laporan hasil pengujian ketahanan keamanan siber berbasis skenario termasuk hasil kaji ulang yang telah dilakukan kepada OJK. Laporan tersebut paling sedikit mencakup ringkasan pelaksanaan pengujian, *lesson learned* atau hasil observasi dari hasil pengujian, dan rencana atau perbaikan yang telah dilakukan. Laporan tersebut harus disampaikan paling

lambat 10 (sepuluh) hari kerja setelah dilaksanakannya pengujian ketahanan keamanan siber berbasis skenario tersebut.

138. Dalam hal berdasarkan penilaian tingkat maturitas manajemen risiko keamanan siber yang dilakukan oleh Bank terdapat tingkat maturitas manajemen risiko keamanan siber yang masuk peringkat 4 atau 5, maka Direksi dan Dewan Komisaris Bank harus menyampaikan rencana tindak (*action plan*) kepada OJK. Rencana tindak tersebut harus disampaikan paling lambat 10 (sepuluh) hari kerja setelah hasil penilaian oleh Bank.

Lampiran A – Format Laporan Insiden Siber

Laporan	Keterangan
Notifikasi Insiden Awal	• Bank melengkapi Format Laporan Notifikasi Insiden Awal sebagaimana Bagian A kepada OJK secepatnya paling lambat 1x24 jam setelah insiden diketahui.
Pengkinian Notifikasi Insiden Awal	• Bank melakukan pengkinian atas Format Laporan Notifikasi Insiden Awal sebagaimana Bagian A dalam hal terdapat perubahan kondisi atau atas permintaan OJK.
Laporan Pengkinian Insiden	• Bank melengkapi Format Laporan Insiden secara lengkap sebagaimana Bagian A dan B secara bulanan.

Bagian (A) Laporan Notifikasi Insiden Awal	
1. Informasi Pelaporan:	
• Tanggal dan Waktu Notifikasi kepada OJK	
• Nama Bank	
• Nama Pelapor	
• Departemen/Divisi Pelapor	
• Kontak Pelapor	
2. Detail Insiden:	
• Tanggal dan Waktu Diketahuinya Insiden	
• Jenis insiden: (i) **<u>Serangan Siber</u>** *(Hacking* atau *Cracking, virus, malware,* atau *ransomware, skimming, phising, social engineering, web defacement, distributed denial of service attacks,* dll) (ii) **<u>Pencurian atau Kehilangan Data/ Informasi</u>** (iii) **<u>Kejadian siber lainnya</u>** yang dapat membahayakan keamanan atas sistem informasi atau melanggar kebijakan, prosedur, atau kebijakan penggunaan keamanan siber.	

• Tindakan awal penanganan yang telah dilakukan bank	
3. Penilaian Dampak Insiden (dapat termasuk namun tidak terbatas sebagaimana contoh terlampir):	
• Dampak terhadap bisnis termasuk ketersedian dan opernasional layanan bank – misalnya Layanan *Treasury*, *Cash Management, Trade Finance*, ATM, *Internet Banking, Mobile Banking*, Aktivitas Kliring dll.	
• Dampak terhadap pihak ketiga – pengaruh terhadap nasabah baik retail maupun korporasi, *service providers* dll.	
• Dampak terhadap financial dan market – nilai dan volume transaksi, kerugian materiil, dampak terhadap likuiditas, *bank run*, penarikan dana, dll.	
• Dampak reputasi bank – Potensi insiden menarik perhatian media	
• Dampak terhadap aspek hukum dan peraturan perundang-undangan.	
Bagian (B) Laporan Insiden Berkala	
4. Detail Kronologis Insiden:	
• Tanggal, waktu, dan durasi terjadinya insiden.	
• Langkah eskalasi dan mitigasi yang dilakukan, sesuai dengan rencana penanganan dan pemulihan bank.	
• Keterlibatan pihak ketiga	
• Detail langkap komunikasi yang dilakukan bank	
5. Analisis *Root Cause* Insiden:	
• Faktor penyebab insiden	
• Tindak lanjut penyelesaian insiden, sesuai dengan rencana penanganan dan pemulihan bank	
• Langkah perbaikan yang diidentifikasi bank	
6. Asesmen Final:	

• Kesimpulan atas penyebab dan dampak dari insiden	
• *Corrective actions* yang dapat dilakukan bank untuk mencegah terjadinya insiden yang serupa di masa yang akan datang.	
• Target waktu penyelesaian insiden _____ (DD/MM/YY).	

Lampiran B – Penilaian Tingkat Risiko Keamanan Siber Inheren

Matriks Tingkat Risiko Inheren untuk Risiko Keamanan Siber

Peringkat	Definisi Peringkat
Low (1)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, kemungkinan kerugian yang dihadapi bank dari risiko keamanan siber inheren 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, antara lain dalam aspek komputer, aplikasi, sistem, dan koneksi. Kerentanan terhadap gangguan atau serangan sangat rendah. b. Saluran distribusi (*delivery channel*) yang digunakan bank masih bersifat sangat sederhana dan tidak terdapat eksposur tinggi terhadap internet atau jaringan *online* dan *mobile.* c. Variasi produk, layanan, dan jasa bank yang menggunakan teknologi dan/atau jaringan *online* dan *mobile* sangat terbatas dengan volume transaksi yang sangat rendah. d. 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. e. Frekuensi dan materialitas ancaman 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 keamanan siber inheren 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, antara lain dalam aspek komputer, aplikasi, sistem, dan koneksi. Kerentanan terhadap gangguan atau serangan rendah. Bank melakukan *outsourcing* sistem pada pihak ketiga dengan kompleksitas yang sangat rendah. b. Saluran distribusi (*delivery channel*) yang digunakan bank masih bersifat sederhana dan terdapat eksposur yang relatif rendah terhadap internet atau jaringan *online* dan *mobile.* c. Variasi produk, layanan, dan jasa bank yang menggunakan teknologi dan/atau jaringan *online* dan *mobile* terbatas dengan volume transaksi yang rendah. d. Karakteristik organisasi bank memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank baik. Lokasi operasional bank terbatas. e. Frekuensi dan materialitas ancaman siber bank selama 12 (dua belas) bulan terakhir relatif rendah dan relatif tidak signifikan.
Moderate (3)	Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, kemungkinan kerugian yang dihadapi bank dari risiko keamanan siber inheren 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, antara lain dalam aspek komputer, aplikasi, sistem, dan koneksi. Kerentanan terhadap gangguan atau serangan cukup rendah. Bank melakukan *outsourcing* sistem dan aplikasi yang bersifat kritikal pada pihak ketiga dengan kompleksitas yang rendah. b. Saluran distribusi (*delivery channel*) yang digunakan bank bersifat cukup kompleks dan terdapat eksposur relatif tinggi terhadap internet atau jaringan *online* dan *mobile.* c. Variasi produk, layanan, dan jasa bank yang menggunakan teknologi dan/atau jaringan *online* dan *mobile* cukup terbatas dengan volume transaksi yang cukup rendah. d. Karakteristik organisasi bank cukup memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank cukup baik. Lokasi operasional cukup terbatas.

	e. Frekuensi dan materialitas ancaman 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 keamanan siber inheren 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, antara lain dalam aspek komputer, aplikasi, sistem, dan koneksi. Kerentanan terhadap gangguan atau serangan cukup tinggi. Bank melakukan *outsourcing* sistem dan aplikasi yang bersifat kritikal pada pihak ketiga dengan kompleksitas yang cukup tinggi. b. Saluran distribusi (*delivery channel*) yang digunakan bank bersifat kompleks, misalnya menggunakan banyak teknologi baru (*emerging technologies*), dan terdapat eksposur tinggi terhadap internet atau jaringan *online* dan *mobile.* c. Variasi produk, layanan, dan jasa bank yang menggunakan teknologi dan/atau jaringan *online* dan *mobile* cukup tinggi dengan volume transaksi yang cukup tinggi. d. 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 cukup beragam. e. Frekuensi dan materialitas ancaman 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 keamanan siber inheren 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, antara lain dalam aspek komputer, aplikasi, sistem, dan koneksi. Kerentanan

	terhadap gangguan atau serangan sangat tinggi. Bank melakukan *outsourcing* sistem dan aplikasi yang bersifat kritikal pada pihak ketiga dengan kompleksitas yang tinggi. b. Saluran distribusi (*delivery channel*) yang digunakan bank bersifat sangat kompleks, misalnya menggunakan banyak teknologi baru (*emerging technologies*), dan terdapat eksposur yang sangat tinggi terhadap internet atau jaringan *online* dan *mobile.* c. Variasi produk, layanan, dan jasa bank yang menggunakan teknologi dan/atau jaringan *online* dan *mobile* sangat tinggi dengan volume transaksi yang sangat tinggi. d. Karakteristik organisasi bank tidak memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Lingkungan teknologi informasi bank tidak baik dan mapan. Lokasi operasional sangat tinggi dan beragam. e. Frekuensi dan materialitas ancaman siber bank selama 12 (dua belas) bulan terakhir sangat tinggi dengan dampak yang sangat signifikan.

Lampiran C – Penilaian Tingkat Kualitas Penerapan Manajemen Risiko Keamanan Siber Bank

Matriks Tingkat Kualitas Penerapan Manajemen Risiko Keamanan Siber

Peringkat	Definisi Peringkat
Strong (1)	Kualitas penerapan kematangan keamanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Ban yang termasuk dalam peringkat *Advanced* (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 keamanan siber bank. c. Struktur organisasi terkait penerapan manajemen risiko 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 keamanan siber. e. Budaya dan kesadaran manajemen risiko 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 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 keamanan siber sangat sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko keamanan siber.

	i. Kebijakan dan prosedur manajemen risiko serta penetapan limit risiko keamanan siber sangat memadai dan tersedia untuk seluruh area manajemen risiko keamanan siber, sejalan dengan penerapan, dan dipahami dengan baik oleh pegawai. j. Proses identifikasi dalam manajemen risiko keamanan siber sangat memadai. k. Proses perlindungan dalam manajemen risiko keamanan siber dilaksanakan dengan sangat baik. l. Proses deteksi dalam ketanggapan manajemen risiko keamanan siber sangat andal dan teruji. m. Proses ketahanan dalam menanggulangi insiden siber dilaksanakan dengan sangat baik dan tidak menimbulkan gangguan yang signifikan. n. Sistem informasi manajemen risiko keamanan siber sangat baik sehingga menghasilkan laporan risiko keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris. o. Sistem pengendalian intern sangat efektif dalam mendukung pelaksanaan manajemen risiko keamanan siber. p. 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. q. Secara umum tidak terdapat kelemahan yang signifikan berdasarkan hasil kaji ulang independen. r. Tindak lanjut atas kaji ulang independen telah dilaksanakan dengan sangat memadai.
Satisfactory (2)	Kualitas penerapan kematangan keamanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat *Managed* (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 keamanan siber bank. c. Struktur organisasi terkait penerapan manajemen risiko 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 keamanan siber. e. Budaya dan kesadaran manajemen risiko 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 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 keamanan siber sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko keamanan siber. i. Kebijakan dan prosedur manajemen risiko serta penetapan limit risiko keamanan siber memadai dan tersedia untuk seluruh area manajemen risiko keamanan siber, sejalan dengan penerapan, dan dipahami dengan baik oleh pegawai meskipun terdapat kelemahan minor. j. Proses identifikasi dalam manajemen risiko keamanan siber memadai. k. Proses perlindungan dalam manajemen risiko keamanan siber dilaksanakan dengan baik. l. Proses deteksi dalam ketanggapan manajemen risiko keamanan siber andal dan teruji. m. Proses ketahanan dalam menanggulangi insiden siber dilaksanakan dengan baik meskipun terdapat gangguan namun tidak bersifat signifikan. n. Sistem informasi manajemen risiko keamanan siber baik, termasuk pelaporan risiko keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris. o. Sistem pengendalian intern efektif dalam mendukung pelaksanaan manajemen risiko keamanan siber. p. 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. q. Terdapat kelemahan yang tidak signifikan berdasarkan hasil kaji ulang independen. r. Tindak lanjut atas kaji ulang independen telah dilaksanakan dengan memadai.

Fair (3)	Kualitas penerapan kematangan keamanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat *Intermediate* (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 keamanan siber bank. c. Struktur organisasi terkait penerapan manajemen risiko 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 keamanan siber. e. Budaya dan kesadaran manajemen risiko 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 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 keamanan siber cukup sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko keamanan siber. i. Kebijakan dan prosedur manajemen risiko serta penetapan limit risiko keamanan siber cukup memadai namun tidak selalu sejalan dengan penerapan. j. Proses identifikasi dalam manajemen risiko keamanan siber cukup memadai. k. Proses perlindungan dalam manajemen risiko keamanan siber dilaksanakan dengan cukup baik. l. Proses deteksi dalam ketanggapan manajemen risiko keamanan siber cukup andal dan teruji. m. Proses ketahanan dalam menanggulangi insiden siber dilaksanakan dengan cukup baik namun tetap menimbulkan gangguan yang bersifat minor.

	n. Sistem informasi manajemen risiko keamanan siber cukup baik, termasuk pelaporan risiko keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris. o. Sistem pengendalian intern cukup efektif dalam mendukung pelaksanaan manajemen risiko keamanan siber. p. 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. q. Terdapat kelemahan yang cukup signifikan berdasarkan hasil kaji ulang independen yang memerlukan perhatian manajemen. r. Tindak lanjut atas kaji ulang independen telah dilaksanakan dengan cukup memadai
Marginal (4)	Kualitas penerapan kematangan keamanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat *Evolving* (4) antara lain sebagai berikut: a. Pengawasan aktif Direksi dan Dewan Komisaris secara keseluruhan kurang memadai. Tredapat kelemahan pada berbagai aspek penilaian yang memerlukan perbaikan segera. b. Sumber daya manusia kurang memadai dari sisi kuantitas maupun kompetensi pada fungsi manajemen risiko keamanan siber bank. c. Struktur organisasi terkait penerapan manajemen risiko 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 keamanan siber. e. Budaya dan kesadaran manajemen risiko 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 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 keamanan siber kurang sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko keamanan siber. i. Kebijakan dan prosedur manajemen risiko serta penetapan limit risiko keamanan siber kurang memadai dan tidak sejalan dengan penerapan. j. Proses identifikasi dalam manajemen risiko keamanan siber kurang memadai. k. Proses perlindungan dalam manajemen risiko keamanan siber dilaksanakan dengan kurang baik. l. Proses deteksi dalam ketanggapan manajemen risiko keamanan siber kurang andal dan teruji. m. Proses ketahanan dalam menanggulangi insiden siber kurang dilaksanakan dengan baik dan menimbulkan gangguan yang signifikan. n. Kelemahan signifikan pada sistem informasi manajemen risiko keamanan siber, termasuk pelaporan risiko keamanan siber yang komprehensif dan terintegrasi kepada Direksi dan Dewan Komisaris yang memerlukan perbaikan segera. o. Sistem pengendalian intern kurang efektif dalam mendukung pelaksanaan manajemen risiko keamanan siber. p. 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. q. Terdapat kelemahan yang signifikan berdasarkan hasil kaji ulang independen yang memerlukan perbaikan segera. r. Tindak lanjut atas kaji ulang independen kurang memadai.
Unsatisfactory (5)	Kualitas penerapan kematangan keamanan siber sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat *Initial* (5) antara lain sebagai berikut:

	a. Pengawasan aktif Direksi dan Dewan Komisaris tidak memadai. Tredapat 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 keamanan siber bank. c. Struktur organisasi terkait penerapan manajemen risiko keamanan siber pada seluruh satuan kerja tidak berjalan dengan baik. d. Kesadaran *(awareness)* dan pemahaman Direksi dan Dewan Komisaris sangat lemah mengenai manajemen risiko keamanan siber. e. Budaya dan kesadaran manajemen risiko 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 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 keamanan siber tidak sejalan dengan tingkat risiko yang akan diambil dan toleransi risiko keamanan siber. i. Kelemahan sangat signifikan pada kebijakan dan prosedur manajemen risiko serta penetapan limit risiko keamanan siber. j. Proses identifikasi dalam manajemen risiko keamanan siber tidak memadai. k. Proses perlindungan dalam manajemen risiko keamanan siber tidak dilaksanakan dengan baik. l. Proses deteksi dalam ketanggapan manajemen risiko keamanan siber tidak andal dan teruji. m. Proses ketahanan dalam menanggulangi insiden siber tidak dilaksanakan dengan baik sehingga menimbulkan gangguan yang sangat signifikan. n. Kelemahan fundamental pada sistem informasi manajemen risiko keamanan siber. o. Sistem pengendalian intern tidak efektif dalam mendukung pelaksanaan manajemen risiko keamanan siber.

	p. 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. q. Terdapat kelemahan yang sangat signifikan berdasarkan hasil kaji ulang independen yang memerlukan perbaikan segera. r. Tindak lanjut atas kaji ulang independen tidak memadai atau tidak ada.

Lampiran D – Penilaian Tingkat Maturitas Manajemen Risiko Keamanan Siber Bank

Matriks Tingkat Maturitas Manajemen Risiko Keamanan Siber

Peringkat	Definisi Peringkat
Strong (1)	Tingkat maturitas manajemen risiko keamanan siber bank yang termasuk dalam peringkat ini pada umumnya memiliki karakteristik antara lain sebagai berikut: a. Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, risiko keamanan siber inheren tergolong sangat rendah selama periode waktu tertentu pada masa datang. b. Kualitas penerapan manajemen risiko keamanan siber sangat memadai. Dalam hal terdapat kelemahan minor, kelemahan tersebut dapat diabaikan.
Managed (2)	Tingkat maturitas manajemen risiko keamanan siber bank yang termasuk dalam peringkat ini pada umumnya memiliki karakteristik antara lain sebagai berikut: a. Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, risiko keamanan siber inheren tergolong rendah selama periode waktu tertentu pada masa datang. b. Kualitas penerapan manajemen risiko keamanan siber memadai. Dalam hal terdapat kelemahan minor, kelemahan tersebut perlu mendapatkan perhatian manajemen.
Intermediate (3)	Tingkat maturitas manajemen risiko keamanan siber bank yang termasuk dalam peringkat ini pada umumnya memiliki karakteristik antara lain sebagai berikut: a. Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, risiko keamanan siber inheren tergolong cukup tinggi selama periode waktu tertentu pada masa datang. b. Kualitas penerapan manajemen risiko keamanan siber cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen dan perbaikan.

Evolving (4)	Tingkat maturitas manajemen risiko keamanan siber bank yang termasuk dalam peringkat ini pada umumnya memiliki karakteristik antara lain sebagai berikut: a. Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, risiko keamanan siber inheren tergolong tinggi selama periode waktu tertentu pada masa datang. b. Kualitas penerapan manajemen risiko keamanan siber kurang memadai. Terdapat kelemahan signifikan pada berbagai aspek manajemen risiko yang membutuhkan tindakan korektif segera.
Baseline (5)	Tingkat maturitas manajemen risiko keamanan siber bank yang termasuk dalam peringkat ini pada umumnya memiliki karakteristik antara lain sebagai berikut: a. Dengan mempertimbangkan aktivitas bisnis yang dilakukan bank, risiko keamanan siber inheren tergolong sangat tinggi selama periode waktu tertentu pada masa datang. b. Kualitas penerapan manajemen risiko keamanan siber tidak memadai. Terdapat kelemahan signifikan pada berbagai aspek manajemen risiko yang tindakan penyelesaiannya di luar kemampuan manajemen.