PERATURAN ANGGOTA DEWAN GUBERNUR
NOMOR 24 TAHUN 2024
TENTANG
KEAMANAN SISTEM INFORMASI DAN KETAHANAN SIBER BAGI PENYELENGGARA SISTEM PEMBAYARAN, PELAKU PASAR UANG DAN PASAR VALUTA ASING, SERTA PIHAK LAIN YANG DIATUR DAN DIAWASI BANK INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

ANGGOTA DEWAN GUBERNUR BANK INDONESIA,

Menimbang : a. bahwa Bank Indonesia telah menerbitkan Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia yang perlu didukung dengan peraturan pelaksanaan teknis sebagai pedoman penerapan keamanan sistem informasi dan ketahanan siber yang konsisten, efektif, dan terukur;

b. bahwa pedoman penerapan keamanan sistem informasi dan ketahanan siber yang konsisten, efektif, dan terukur diperlukan untuk mendorong penyelenggara agar mampu mengidentifikasi, mencegah, dan merespons ancaman siber atau serangan siber;

c. bahwa upaya untuk mengidentifikasi, mencegah, dan merespons ancaman siber atau serangan siber ditujukan untuk penguatan keamanan sistem informasi dan ketahanan siber di sektor keuangan;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Anggota Dewan Gubernur tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia;

Mengingat : Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi

Bank Indonesia (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 9/BI, Tambahan Lembaran Negara Republik Indonesia Nomor 77/BI);

MEMUTUSKAN:

Menetapkan : PERATURAN ANGGOTA DEWAN GUBERNUR TENTANG KEAMANAN SISTEM INFORMASI DAN KETAHANAN SIBER BAGI PENYELENGGARA SISTEM PEMBAYARAN, PELAKU PASAR UANG DAN PASAR VALUTA ASING, SERTA PIHAK LAIN YANG DIATUR DAN DIAWASI BANK INDONESIA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Anggota Dewan Gubernur ini yang dimaksud dengan:

1. Sistem Informasi adalah keterpaduan antara komponen data, informasi, sistem aplikasi, infrastruktur teknologi informasi, proses, dan/atau manusia yang saling berinteraksi untuk mencapai suatu tujuan.
2. Siber adalah ruang yang bersifat virtual yang dibentuk dari Sistem Informasi.
3. Sistem Pembayaran adalah suatu sistem yang mencakup seperangkat aturan, lembaga, mekanisme, infrastruktur, sumber dana untuk pembayaran, dan akses ke sumber dana untuk pembayaran, yang digunakan untuk melaksanakan pemindahan dana guna memenuhi suatu kewajiban yang timbul dari suatu kegiatan ekonomi.
4. Sistem Keuangan adalah suatu kesatuan yang terdiri atas lembaga jasa keuangan, pasar keuangan, dan infrastruktur keuangan, termasuk Sistem Pembayaran, yang berinteraksi dalam memfasilitasi pengumpulan dana masyarakat dan pengalokasiannya untuk mendukung aktivitas perekonomian nasional, serta korporasi dan rumah tangga yang terhubung dengan lembaga jasa keuangan.
5. Pasar Uang adalah bagian dari Sistem Keuangan yang berkaitan dengan:
   a. kegiatan penerbitan dan perdagangan instrumen keuangan atau efek bersifat utang yang berjangka waktu tidak lebih dari 1 (satu) tahun;
   b. transaksi pinjam-meminjam uang;
   c. transaksi derivatif suku bunga; dan
   d. transaksi lainnya yang memenuhi karakteristik di Pasar Uang,

   dalam mata uang rupiah atau valuta asing.
6. Pasar Valuta Asing adalah bagian dari Sistem Keuangan yang berkaitan dengan kegiatan transaksi yang melibatkan pertukaran mata uang dari 2 (dua) negara yang berbeda beserta derivatifnya, tetapi tidak termasuk penukaran *bank notes* yang diselenggarakan oleh kegiatan usaha penukaran valuta asing.
7. Penyedia Jasa Pembayaran yang selanjutnya disingkat PJP adalah sebagaimana dimaksud dalam Peraturan Bank Indonesia mengenai Penyedia Jasa Pembayaran.

8. Penyelenggara Infrastruktur Sistem Pembayaran yang selanjutnya disebut PIP adalah pihak yang menyelenggarakan infrastruktur sebagai sarana yang dapat digunakan untuk melakukan pemindahan dana bagi kepentingan anggotanya.
9. Pelaku Usaha Sektor Keuangan yang Bergerak di Pasar Uang dan/atau Pasar Valuta Asing yang selanjutnya disebut PUSK PUVA adalah pelaku usaha di Pasar Uang dan/atau Pasar Valuta Asing yang memperoleh izin kelembagaan dari Bank Indonesia.
10. Lembaga Pendukung Pasar Uang adalah pihak yang memberikan jasa terkait penerbitan instrumen Pasar Uang, perantara pelaksanaan transaksi instrumen Pasar Uang, penyelesaian transaksi, penatausahaan instrumen dan transaksi Pasar Uang, dan pihak lainnya yang ditetapkan oleh Bank Indonesia.
11. Lembaga Pendukung Pasar Valuta Asing adalah pihak yang dapat memberikan jasa terkait perantara pelaksanaan transaksi, penyelesaian transaksi, penatausahaan transaksi di Pasar Valuta Asing, dan pihak lainnya yang ditetapkan oleh Bank Indonesia.
12. Penyelenggara Kegiatan Usaha Penukaran Valuta Asing Bukan Bank adalah sebagaimana dimaksud dalam Peraturan Bank Indonesia mengenai Kegiatan Usaha Penukaran Valuta Asing Bukan Bank.
13. Penyelenggara adalah pihak yang diatur dan diawasi Bank Indonesia yang mempunyai risiko Siber baik secara sistemik maupun nonsistemik bagi Sistem Keuangan.
14. Kerentanan Siber adalah kelemahan, kerawanan, atau kekurangan yang terdapat pada Siber sehingga berdampak negatif terhadap bisnis dan/atau layanan operasional Penyelenggara.
15. Ancaman Siber adalah suatu keadaan yang berpotensi mengeksploitasi Kerentanan Siber.
16. Serangan Siber adalah upaya untuk mengeksploitasi Kerentanan Siber.
17. Insiden Siber adalah Serangan Siber yang mengganggu kelancaran bisnis dan/atau layanan operasional Penyelenggara yang memerlukan respons dan/atau pemulihan.
18. Risiko Siber adalah kemungkinan terjadinya Insiden Siber dan dampak yang diakibatkan dari Insiden Siber.
19. Keamanan Sistem Informasi dan Ketahanan Siber yang selanjutnya disebut KKS adalah kondisi terjaganya kerahasiaan, keutuhan, serta ketersediaan informasi dan/atau Sistem Informasi Penyelenggara dari Serangan Siber dan terjaganya kelangsungan bisnis Penyelenggara melalui tindakan antisipatif, adaptif, dan proaktif terhadap Ancaman Siber serta kemampuan Penyelenggara untuk melakukan respons dan pemulihan dengan cepat terhadap Insiden Siber.
20. *Self-Regulatory Organization* yang selanjutnya disingkat SRO adalah suatu forum atau institusi yang berbadan hukum Indonesia yang ditetapkan oleh Bank Indonesia untuk mendukung penyelenggaraan Sistem Pembayaran,

Pasar Uang dan Pasar Valuta Asing, dan/atau kegiatan lainnya yang diatur dan diawasi Bank Indonesia.

BAB II
OBJEK DAN RUANG LINGKUP

Pasal 2

Penyelenggara yang menjadi objek pengaturan dan pengawasan KKS meliputi:
a. PJP;
b. PIP;
c. PUSK PUVA;
d. Lembaga Pendukung Pasar Uang;
e. Lembaga Pendukung Pasar Valuta Asing;
f. Penyelenggara Kegiatan Usaha Penukaran Valuta Asing Bukan Bank; dan
g. pihak lain yang diatur dan diawasi Bank Indonesia.

Pasal 3

Ruang lingkup pengaturan dan pengawasan KKS meliputi:
a. tata kelola;
b. pencegahan;
c. penanganan;
d. penyampaian data dan informasi;
e. tata cara pengenaan sanksi; dan
f. kolaborasi.

BAB III
TATA KELOLA

Bagian Kesatu
Strategi dan Kebijakan KKS

Pasal 4

(1) Strategi dan kebijakan KKS meliputi:
    a. rencana strategis KKS;
    b. kebijakan, standar, dan prosedur KKS; dan
    c. fungsi organisasi KKS.
(2) Strategi dan kebijakan KKS sebagaimana dimaksud pada ayat (1) disusun dan dilaksanakan oleh Penyelenggara untuk memperkuat KKS.

Paragraf 1
Rencana Strategis KKS

Pasal 5

(1) Rencana strategis KKS sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a meliputi:
    a. arah strategis penguatan KKS;
    b. peta jalan penguatan KKS; dan
    c. perkiraan kebutuhan sumber daya,
    yang mencakup aspek manusia, proses, dan teknologi.
(2) Arah strategis penguatan KKS sebagaimana dimaksud pada ayat (1) huruf a disusun dengan memperhatikan:
    a. arah dan rencana strategis bisnis Penyelenggara;
    b. selera risiko Penyelenggara;

c. ketentuan peraturan perundang-undangan mengenai KKS; dan/atau
d. perkembangan tren teknologi, Kerentanan Siber, dan Ancaman Siber.

(3) Peta jalan penguatan KKS sebagaimana dimaksud pada ayat (1) huruf b disusun sesuai dengan arah strategis penguatan KKS yang paling sedikit mencakup:
a. daftar program dan/atau proyek;
b. jadwal dan tahapan;
c. hasil kerja; dan
d. pelaksana.

(4) Perkiraan kebutuhan sumber daya sebagaimana dimaksud pada ayat (1) huruf c disusun untuk melaksanakan peta jalan penguatan KKS yang mencakup perkiraan biaya dan sumber daya manusia.

Pasal 6

(1) Rencana strategis KKS sebagaimana dimaksud dalam Pasal 5 ayat (1) ditetapkan oleh manajemen tertinggi Penyelenggara.

(2) Pemantauan pelaksanaan peta jalan penguatan KKS sebagaimana dimaksud dalam Pasal 5 ayat (3) dilakukan agar pencapaian sesuai dengan jadwal dan tahapan yang ditetapkan.

(3) Evaluasi terhadap rencana strategis KKS sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan memperhatikan perkembangan Risiko Siber.

Paragraf 2
Kebijakan, Standar, dan Prosedur KKS

Pasal 7

(1) Kebijakan, standar, dan prosedur KKS sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b mencakup aspek manusia, proses, dan teknologi yang paling sedikit terdiri atas:
a. pengamanan data, sistem aplikasi, dan infrastruktur teknologi informasi;
b. pengamanan pihak ketiga; dan
c. pelindungan konsumen dan manajemen *fraud*.

(2) Kebijakan, standar, dan prosedur KKS sebagaimana dimaksud pada ayat (1) disusun dengan memperhatikan:
a. rencana strategis KKS;
b. kompleksitas Sistem Informasi; dan
c. profil risiko.

(3) Kebijakan KKS sebagaimana dimaksud pada ayat (1) ditetapkan oleh manajemen tertinggi Penyelenggara.

(4) Standar dan prosedur KKS sebagaimana dimaksud pada ayat (1) disusun untuk mendukung pelaksanaan kebijakan KKS.

(5) Kebijakan, standar, dan prosedur KKS sebagaimana dimaksud pada ayat (1) diterapkan dan dikomunikasikan kepada seluruh pihak internal dan/atau pihak ketiga terkait.

(6) Evaluasi terhadap kebijakan, standar, dan prosedur KKS sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Paragraf 3
Fungsi Organisasi KKS

Pasal 8

(1) Fungsi organisasi KKS sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c meliputi:
   a. manajemen KKS;
   b. manajemen Risiko Siber; dan
   c. audit KKS.
(2) Dalam menjalankan fungsi organisasi KKS sebagaimana dimaksud pada ayat (1), Penyelenggara memperhatikan:
   a. efektivitas dan efisiensi;
   b. akuntabilitas; dan
   c. kapasitas dan kapabilitas sumber daya manusia.
(3) Fungsi organisasi KKS sebagaimana dimaksud pada ayat (1) harus memiliki peran dan tanggung jawab yang jelas.

Pasal 9

(1) Penerapan manajemen KKS sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf a meliputi:
   a. perencanaan strategis KKS;
   b. penyusunan kebijakan, standar, dan prosedur KKS;
   c. penerapan budaya KKS; dan
   d. pelaksanaan pencegahan dan penanganan KKS.
(2) Manajemen KKS sebagaimana dimaksud pada ayat (1) bertanggung jawab pada manajemen tertinggi.
(3) Penerapan manajemen KKS sebagaimana dimaksud pada ayat (1) dilakukan dengan memastikan personel memiliki pengetahuan dan pengalaman yang relevan.
(4) Dalam penerapan manajemen KKS sebagaimana dimaksud pada ayat (1), manajemen KKS dapat bekerja sama dengan pihak lain dengan mempertimbangkan Risiko Siber.
(5) Dalam penerapan manajemen KKS sebagaimana dimaksud pada ayat (1), evaluasi dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 10

(1) Penerapan manajemen Risiko Siber sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf b dilakukan paling sedikit melalui:
   a. integrasi manajemen Risiko Siber ke dalam proses manajemen risiko Penyelenggara;
   b. identifikasi, asesmen, mitigasi, dan evaluasi Risiko Siber terhadap Ancaman Siber atau Serangan Siber; dan
   c. pengukuran tingkat kematangan KKS.
(2) Pengukuran tingkat kematangan KKS sebagaimana dimaksud pada ayat (1) huruf c paling sedikit mencakup:
   a. tata kelola;
   b. pencegahan; dan
   c. penanganan.

(3) Pengukuran tingkat kematangan KKS sebagaimana dimaksud pada ayat (1) huruf c menghasilkan nilai dan kategori tingkat kematangan KKS.
(4) Hasil pengukuran tingkat kematangan KKS sebagaimana dimaksud pada ayat (3) disampaikan kepada manajemen tertinggi Penyelenggara.

Pasal 11

Audit KKS sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf c paling sedikit mencakup:
a. tata kelola;
b. pencegahan; dan
c. penanganan.

Pasal 12

(1) Audit KKS sebagaimana dimaksud dalam Pasal 11 dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(2) Audit KKS sebagaimana dimaksud pada ayat (1) dilakukan oleh pihak internal dan/atau eksternal secara independen.
(3) Pihak eksternal yang melaksanakan audit KKS merupakan auditor KKS independen yang terdaftar di SRO dan/atau otoritas lain.
(4) Hasil audit KKS sebagaimana dimaksud pada ayat (2) disampaikan kepada manajemen tertinggi Penyelenggara dan digunakan untuk perbaikan tata kelola, pencegahan, dan penanganan.

Bagian Kedua
Budaya KKS

Pasal 13

(1) Budaya KKS dilaksanakan oleh Penyelenggara melalui program peningkatan budaya KKS.
(2) Program peningkatan budaya KKS sebagaimana dimaksud pada ayat (1) meliputi:
    a. kesadaran (*awareness*);
    b. pelatihan; dan/atau
    c. edukasi.
(3) Program peningkatan budaya KKS sebagaimana dimaksud pada ayat (2) diberikan kepada:
    a. pihak internal;
    b. pihak ketiga; dan
    c. konsumen.
(4) Program peningkatan budaya KKS sebagaimana dimaksud pada ayat (2) dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan melibatkan manajemen tertinggi sebagai teladan.
(5) Program peningkatan budaya KKS sebagaimana dimaksud pada ayat (2) diselaraskan dengan rencana strategis KKS.
(6) Evaluasi terhadap program peningkatan budaya KKS sebagaimana dimaksud pada ayat (2) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

BAB IV
PENCEGAHAN

Bagian Kesatu
Identifikasi

Pasal 14

(1) Identifikasi meliputi:
    a. penyusunan profil Risiko Siber; dan
    b. penginian profil Risiko Siber secara berkala.
(2) Penyusunan profil Risiko Siber sebagaimana dimaksud pada ayat (1) huruf a meliputi:
    a. identifikasi Risiko Siber;
    b. asesmen Risiko Siber; dan
    c. analisis dampak bisnis.
(3) Penginian profil Risiko Siber sebagaimana dimaksud pada ayat (1) huruf b dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(4) Dalam hal terjadi Insiden Siber, Penyelenggara melakukan penginian profil Risiko Siber.

Paragraf 1
Identifikasi Risiko Siber

Pasal 15

(1) Identifikasi Risiko Siber sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a dilakukan dengan memperhatikan paling sedikit:
    a. Kerentanan Siber dan Ancaman Siber dari aspek manusia, proses, dan teknologi; dan
    b. objek yang akan dilindungi.
(2) Kerentanan Siber dan Ancaman Siber sebagaimana dimaksud pada ayat (1) huruf a dapat bersumber dari:
    a. internal; dan
    b. eksternal.
(3) Informasi Kerentanan Siber dan Ancaman Siber sebagaimana dimaksud pada ayat (2) dapat bersumber dari sarana pertukaran informasi yang dibentuk Bank Indonesia atau sarana informasi lain.
(4) Objek yang akan dilindungi sebagaimana dimaksud pada ayat (1) huruf b yaitu Sistem Informasi yang digunakan oleh Penyelenggara baik yang dikelola Penyelenggara atau pihak lain.
(5) Hasil identifikasi Risiko Siber sebagaimana dimaksud pada ayat (1) didokumentasikan pada inventaris risiko (*risk register*) di tingkat organisasi Penyelenggara.

Paragraf 2
Asesmen Risiko Siber

Pasal 16

(1) Asesmen Risiko Siber sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b dilakukan paling sedikit dengan:
    a. menentukan metodologi asesmen Risiko Siber yang relevan;

b. melakukan penilaian dampak Kerentanan Siber dan Ancaman Siber yang memengaruhi layanan operasional; dan
c. melakukan prioritisasi mitigasi terhadap Kerentanan Siber dan Ancaman Siber mulai dari yang paling tinggi sampai dengan yang paling rendah.

(2) Metodologi asesmen Risiko Siber sebagaimana dimaksud pada ayat (1) huruf a mencakup penilaian dampak (*impact*) yang ditimbulkan dari Risiko Siber dan penilaian kemungkinan terjadinya Risiko Siber (*likelihood*).

(3) Penyelenggara memastikan metodologi asesmen Risiko Siber sebagaimana dimaksud pada ayat (1) huruf a dapat memperoleh hasil asesmen Risiko Siber yang konsisten dan valid.

(4) Penilaian dampak Kerentanan Siber dan Ancaman Siber yang memengaruhi layanan operasional sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan mengukur perkiraan:
a. kerugian sebagai akibat dari gangguan layanan;
b. dampak kerusakan; dan
c. biaya pemulihan.

(5) Prioritisasi mitigasi terhadap Kerentanan Siber dan Ancaman Siber mulai dari yang paling tinggi sampai dengan yang paling rendah sebagaimana dimaksud pada ayat (1) huruf c dilakukan berdasarkan:
a. tingkat Risiko Siber;
b. urgensi waktu pelaksanaan mitigasi Risiko Siber; dan
c. urutan pelaksanaan mitigasi Risiko Siber.

Paragraf 3
Analisis Dampak Bisnis

Pasal 17

(1) Analisis dampak bisnis sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c dilakukan paling sedikit dengan:
a. melakukan penilaian dampak bisnis terkait Kerentanan Siber terhadap finansial dan nonfinansial, termasuk dampaknya pada stabilitas Sistem Keuangan;
b. menganalisis kritikalitas fungsi bisnis dan Sistem Informasi beserta prioritisasi pengendalian risiko; dan
c. menganalisis Sistem Informasi kritikal yang berdampak luas terhadap stabilitas Sistem Keuangan.

(2) Penilaian dampak bisnis sebagaimana dimaksud pada ayat (1) huruf a dilakukan dengan:
a. menetapkan jenis dan kriteria dampak;
b. menetapkan *maximum tolerable period of disruption*; dan
c. menetapkan sumber daya untuk mendukung fungsi bisnis yang diprioritaskan.

(3) Analisis kritikalitas sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan:
a. menetapkan sasaran waktu pemulihan dan titik pemulihan; dan

b. menetapkan *service level* dan *maximum downtime* yang tidak terjadwal.

(4) Analisis Sistem Informasi kritikal yang berdampak luas terhadap stabilitas sistem keuangan sebagaimana dimaksud pada ayat (1) huruf c dilaksanakan dengan melakukan inventarisasi sistem aplikasi dan/atau infrastruktur teknologi informasi terkait pelaksanaan kegiatan Sistem Pembayaran, Pasar Uang dan Pasar Valuta Asing, serta kegiatan usaha penukaran valuta asing bukan bank.

Pasal 18

Hasil analisis Sistem Informasi kritikal sebagaimana dimaksud dalam Pasal 17 ayat (4) digunakan sebagai pertimbangan dalam mengategorikan infrastruktur informasi vital.

Bagian Kedua
Proteksi

Pasal 19

(1) Proteksi meliputi:
   a. pembangunan sistem pertahanan; dan
   b. pengamanan dan pelindungan data dan/atau informasi.

(2) Evaluasi terhadap penerapan proteksi sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Paragraf 1
Pembangunan Sistem Pertahanan

Pasal 20

Pembangunan sistem pertahanan sebagaimana dimaksud dalam Pasal 19 ayat (1) huruf a pada aspek manusia, proses, dan teknologi dilakukan paling sedikit dengan:

a. memastikan keamanan pihak internal dan pihak ketiga pada setiap tahapan siklus kerja serta memberikan edukasi KKS sesuai dengan peran dan tanggung jawab;
b. menerapkan pengendalian keamanan untuk proses bisnis serta melaksanakan kebijakan, standar, dan prosedur pengamanan secara efektif; dan
c. mengimplementasikan konfigurasi pengamanan terhadap Sistem Informasi yang digunakan.

Pasal 21

(1) Keamanan pihak internal dan pihak ketiga sebagaimana dimaksud dalam Pasal 20 huruf a dipastikan dengan:
   a. memeriksa latar belakang personel pihak internal dan/atau pihak ketiga yang akan dipekerjakan;
   b. mengomunikasikan peran dan tanggung jawab KKS kepada personel pihak internal dan/atau pihak ketiga yang dipekerjakan;
   c. mewajibkan personel pihak internal dan/atau pihak ketiga telah menandatangani perjanjian atau surat pernyataan untuk menjaga kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang;

d. menerapkan pemisahan tugas yang dapat menimbulkan konflik kepentingan dalam pelaksanaan peran dan tanggung jawab personel pihak internal dan/atau pihak ketiga; dan
e. melaksanakan alih pengetahuan dalam hal terdapat perpindahan tanggung jawab atau penonaktifan personel pihak internal dan/atau pihak ketiga.

(2) Kewajiban personel pihak internal dan/atau pihak ketiga menjaga kerahasiaan data dan/atau informasi dari pihak yang tidak berwenang sebagaimana dimaksud pada ayat (1) huruf c dilakukan selama personel dipekerjakan, saat terjadi perpindahan tanggung jawab, dan saat dinonaktifkan.

(3) Pemberian edukasi KKS sesuai dengan peran dan tanggung jawab sebagaimana dimaksud dalam Pasal 20 huruf a dilakukan melalui program peningkatan budaya KKS sebagaimana dimaksud dalam Pasal 13 ayat (2).

Pasal 22

Penerapan pengendalian keamanan untuk proses bisnis sebagaimana dimaksud dalam Pasal 20 huruf b meliputi:
a. manajemen akses logis dan fisik terhadap sistem aplikasi dan infrastruktur teknologi informasi;
b. manajemen perubahan konfigurasi sistem aplikasi dan infrastruktur teknologi informasi;
c. penginian pengendalian keamanan untuk memastikan kecukupan kontrol keamanan;
d. pelindungan yang memadai terhadap KKS dalam perjanjian kerja sama antara Penyelenggara dengan pihak ketiga, termasuk dalam perjanjian penyediaan layanan *cloud*; dan
e. dokumentasi, pengujian, dan pemantauan model kecerdasan artifisial secara berkelanjutan dalam hal menggunakan sistem kecerdasan artifisial.

Pasal 23

Implementasi konfigurasi pengamanan terhadap Sistem Informasi yang digunakan sebagaimana dimaksud dalam Pasal 20 huruf c meliputi:
a. pertahanan perimeter jaringan;
b. pelindungan terhadap ancaman *malware* pada setiap sistem aplikasi;
c. *secure coding* pada pengembangan sistem aplikasi;
d. *patching* dengan menggunakan versi perangkat lunak terkini dan telah teruji;
e. metode otentikasi dan otorisasi sesuai profil Risiko Siber; dan
f. pertahanan terhadap *adversarial attack* pada model kecerdasan artifisial dalam hal menggunakan sistem kecerdasan artifisial.

Paragraf 2
Pengamanan dan Pelindungan Data dan Informasi

Pasal 24

(1) Pengamanan dan pelindungan data dan/atau informasi sebagaimana dimaksud dalam Pasal 19 ayat (1) huruf b dilakukan paling sedikit dengan:
    a. mengamankan data dan/atau informasi pada setiap tahapan siklus hidup data dan/atau informasi berdasarkan klasifikasi data dan/atau informasi yang ditetapkan oleh Penyelenggara; dan
    b. memastikan kepatuhan pelindungan data pribadi sesuai dengan ketentuan peraturan perundang-undangan.
(2) Pengamanan data dan/atau informasi pada setiap tahapan siklus hidup data dan/atau informasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan saat data dan/atau informasi:
    a. diciptakan;
    b. disimpan;
    c. ditransmisikan;
    d. digunakan; dan
    e. dimusnahkan.

Bagian Ketiga
Deteksi

Pasal 25

(1) Deteksi meliputi:
    a. pemantauan;
    b. analisis hasil pemantauan;
    c. analisis Serangan Siber;
    d. analisis kode jahat atau kode tidak sah; dan
    e. pemeliharaan dan pengujian sistem deteksi.
(2) Deteksi sebagaimana dimaksud pada ayat (1) dilaksanakan secara terpusat untuk mempercepat proses deteksi dan respons Kerentanan Siber, Serangan Siber, dan/atau Insiden Siber.
(3) Deteksi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan memastikan ketersediaan:
    a. sumber daya manusia yang kompeten;
    b. standar dan prosedur pelaksanaan; dan
    c. teknologi sebagai alat bantu sistem deteksi.

Paragraf 1
Pemantauan

Pasal 26

Pemantauan sebagaimana dimaksud dalam Pasal 25 ayat (1) huruf a dilakukan paling sedikit dengan:
a. memantau akses logis dan fisik yang berpotensi menimbulkan Serangan Siber;
b. menetapkan indikator ambang batas sebagai pemicu aktivasi sistem peringatan dini; dan
c. melakukan pemindaian Kerentanan Siber,

secara konsisten dan berkelanjutan.

Pasal 27

Pemantauan akses logis dan fisik yang berpotensi menimbulkan Serangan Siber sebagaimana dimaksud dalam Pasal 26 huruf a meliputi:

a. mengidentifikasi pola akses dan/atau aktivitas yang tidak biasa;
b. menerapkan sistem deteksi paling sedikit pada area dan/atau objek kritikal atau vital;
c. mendokumentasikan dan menyimpan hasil pemantauan dalam bentuk catatan akses dan/atau rekaman visual akses; dan
d. memastikan setiap perubahan terhadap akses logis dan fisik serta konfigurasi dikelola melalui manajemen perubahan.

Pasal 28

(1) Indikator ambang batas sebagai pemicu aktivasi sistem peringatan dini sebagaimana dimaksud dalam Pasal 26 huruf b ditetapkan dengan mengacu pada profil Risiko Siber.
(2) Penginian indikator ambang batas sebagai pemicu aktivasi sistem peringatan dini sebagaimana dimaksud pada ayat (1) dilakukan untuk memastikan efektivitas pemantauan Serangan Siber.

Pasal 29

(1) Pemindaian Kerentanan Siber sebagaimana dimaksud dalam Pasal 26 huruf c dilakukan terhadap sistem aplikasi, infrastruktur teknologi informasi, dan data Penyelenggara untuk menemukan Kerentanan Siber.
(2) Pemindaian Kerentanan Siber sebagaimana dimaksud pada ayat (1) dilakukan dengan mengacu pada profil Risiko Siber.
(3) Pemindaian Kerentanan Siber sebagaimana dimaksud pada ayat (1) dilakukan oleh pihak internal dan/atau menggunakan jasa pihak ketiga.
(4) Dalam hal diperlukan, pemindaian Kerentanan Siber sebagaimana dimaksud pada ayat (1) dapat dilakukan terhadap layanan pihak ketiga.
(5) Evaluasi terhadap pemindaian Kerentanan Siber sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Paragraf 2
Analisis Hasil Pemantauan

Pasal 30

Analisis hasil pemantauan sebagaimana dimaksud dalam Pasal 25 ayat (1) huruf b dilakukan paling sedikit dengan:

a. menganalisis catatan aktivitas Siber; dan
b. menganalisis Kerentanan Siber dan potensi Serangan Siber.

Pasal 31

(1) Analisis catatan aktivitas Siber sebagaimana dimaksud dalam Pasal 30 huruf a meliputi:

a. analisis pola aktivitas Siber yang tidak biasa; dan
b. analisis korelasi catatan aktivitas Siber dari seluruh sistem aplikasi dan infrastruktur teknologi informasi.

(2) Pola aktivitas Siber yang tidak biasa sebagaimana dimaksud pada ayat (1) huruf a meliputi:
a. upaya akses tidak sah;
b. upaya peningkatan peran hak akses;
c. perubahan konfigurasi yang mencurigakan; dan
d. upaya lainnya yang berpotensi menjadi Serangan Siber.

Pasal 32

(1) Analisis Kerentanan Siber dan potensi Serangan Siber sebagaimana dimaksud dalam Pasal 30 huruf b dilakukan berdasarkan hasil analisis catatan aktivitas Siber sebagaimana dimaksud dalam Pasal 31 ayat (1).
(2) Analisis Kerentanan Siber dan potensi Serangan Siber sebagaimana dimaksud pada ayat (1) dilakukan dengan:
a. memperhatikan integrasi informasi dari internal dan eksternal Penyelenggara; dan
b. menggunakan *cyber threat intelligence*.

Paragraf 3
Analisis Serangan Siber

Pasal 33

Analisis Serangan Siber sebagaimana dimaksud dalam Pasal 25 ayat (1) huruf c dilakukan paling sedikit dengan:
a. melakukan asesmen terhadap sumber, jenis, dan waktu terjadinya Serangan Siber termasuk *fraud*;
b. melakukan asesmen terhadap dampak Serangan Siber terhadap sistem dan sistem lainnya yang terhubung; dan
c. melakukan eskalasi jika terdapat potensi terjadi Insiden Siber.

Pasal 34

(1) Asesmen sumber, jenis, dan waktu terjadinya Serangan Siber termasuk *fraud* sebagaimana dimaksud dalam Pasal 33 huruf a meliputi analisis:
a. sumber serangan yaitu asal Serangan Siber, profil *threat actor*, dan *indicator of compromise*;
b. jenis Serangan Siber;
c. waktu terjadinya Serangan Siber dan/atau korelasi Serangan Siber dengan kejadian keamanan Siber lain; dan
d. aktivitas *fraud* pada tingkat akun dan transaksi.
(2) Asesmen dampak Serangan Siber terhadap sistem dan sistem lainnya yang terhubung sebagaimana dimaksud dalam Pasal 33 huruf b berupa analisis korelasi catatan aktivitas Siber dari sistem aplikasi dan infrastruktur teknologi informasi terkait.
(3) Asesmen dampak Serangan Siber terhadap sistem dan sistem lainnya yang terhubung sebagaimana dimaksud pada ayat (2) dilakukan dengan memperhatikan profil Risiko Siber.

(4) Eskalasi jika terdapat potensi terjadi Insiden Siber sebagaimana dimaksud dalam Pasal 33 huruf c dilakukan berdasarkan jalur eskalasi pada rencana penanganan dan pemulihan Insiden Siber.

Paragraf 4
Analisis Kode Jahat atau Kode Tidak Sah

Pasal 35

Analisis kode jahat atau kode tidak sah sebagaimana dimaksud dalam Pasal 25 ayat (1) huruf d dilakukan paling sedikit dengan:

a. menganalisis kode jahat atau kode tidak sah yang berpotensi menimbulkan Serangan Siber; dan
b. melakukan eskalasi tindak lanjut dan/atau evaluasi atas deteksi kode jahat atau kode tidak sah.

Pasal 36

Analisis kode jahat atau kode tidak sah yang berpotensi menimbulkan Serangan Siber sebagaimana dimaksud dalam Pasal 35 huruf a meliputi:

a. melakukan klasifikasi kode jahat atau kode tidak sah berdasarkan tingkat Risiko Siber untuk memastikan penanganan yang sesuai dengan tingkat ancaman;
b. memastikan proses analisis dilakukan dalam lingkungan yang aman dan terisolasi untuk memahami karakteristik, tujuan, dan potensi dampak kode jahat atau kode tidak sah tanpa risiko penyebaran lebih lanjut;
c. melakukan pemindaian sistem aplikasi dan/atau infrastruktur teknologi informasi yang terdampak; dan
d. memastikan setiap kode yang dieksekusi pada sistem aplikasi dan/atau infrastruktur teknologi informasi telah dilakukan otorisasi dan tidak disusupi.

Pasal 37

(1) Eskalasi tindak lanjut atas hasil analisis kode jahat atau kode tidak sah sebagaimana dimaksud dalam Pasal 35 huruf b dilakukan berdasarkan jalur eskalasi pada rencana penanganan dan pemulihan Insiden Siber.
(2) Evaluasi atas deteksi kode jahat atau kode tidak sah sebagaimana dimaksud dalam Pasal 35 huruf b dilakukan untuk penguatan deteksi.

Paragraf 5
Pemeliharaan dan Pengujian Sistem Deteksi

Pasal 38

(1) Pemeliharaan dan pengujian sistem deteksi sebagaimana dimaksud dalam Pasal 25 ayat (1) huruf e dilakukan secara berkala paling sedikit dengan memastikan:
    a. sistem pemantauan terpelihara dengan versi perangkat lunak terkini; dan
    b. keandalan sistem pemantauan telah teruji.
(2) Pemeliharaan dan pengujian sistem deteksi secara berkala sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 39

(1) Penyelenggara memastikan penerapan sistem pemantauan terpelihara dengan versi perangkat lunak terkini sebagaimana dimaksud dalam Pasal 38 ayat (1) huruf a sesuai standar yang berlaku di Penyelenggara.
(2) Pembaruan sistem pemantauan sebagaimana dimaksud pada ayat (1) dilakukan segera setelah versi perangkat lunak terkini dirilis dan telah teruji.
(3) Penyelenggara memastikan keandalan sistem pemantauan telah teruji sebagaimana dimaksud dalam Pasal 38 ayat (1) huruf b melalui penilaian:
    a. akurasi sistem deteksi;
    b. kemampuan sistem deteksi dalam merespons Ancaman Siber dan Serangan Siber; dan
    c. kemampuan sistem deteksi dalam memberikan notifikasi secara cepat.

BAB V
PENANGANAN

Bagian Kesatu
Respons

Pasal 40

Respons meliputi:
a. penyusunan rencana penanganan dan pemulihan Insiden Siber;
b. pelaksanaan simulasi dan uji coba penanganan dan pemulihan Insiden Siber;
c. penanganan Insiden Siber; dan
d. pelaksanaan komunikasi tindakan penanganan Insiden Siber.

Paragraf 1
Penyusunan Rencana Penanganan dan
Pemulihan Insiden Siber

Pasal 41

(1) Penyusunan rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 40 huruf a paling sedikit memuat:
    a. penetapan status Insiden Siber;
    b. respons Insiden Siber;
    c. pembatasan dampak; dan
    d. rencana pemulihan yang mempertimbangkan sasaran waktu pemulihan dan sasaran titik pemulihan.
(2) Penetapan status Insiden Siber sebagaimana dimaksud pada ayat (1) huruf a dilakukan berdasarkan kriteria penetapan Insiden Siber.
(3) Dalam hal terjadi Insiden Siber, Penyelenggara menentukan Insiden Siber sesuai kategori yang telah ditetapkan dengan memperhatikan dampak dan prioritas penanganan Insiden Siber.

(4) Respons Insiden Siber sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan memperhatikan sasaran waktu pemulihan dan sasaran titik pemulihan, paling sedikit mencakup:
   a. prosedur penanganan untuk menghilangkan sumber Insiden Siber dan eskalasi untuk setiap kategori Insiden Siber dengan mempertimbangkan kebutuhan analisis *post-mortem*;
   b. daftar personel pihak internal atau pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam penanganan Insiden Siber; dan
   c. daftar sistem aplikasi termasuk aplikasi pendukung, infrastruktur teknologi informasi, dan sumber daya lainnya yang diperlukan dalam penanganan Insiden Siber.

(5) Pembatasan dampak sebagaimana dimaksud pada ayat (1) huruf c paling sedikit mencakup prosedur:
   a. isolasi dampak Insiden Siber di internal Penyelenggara; dan
   b. koordinasi isolasi dampak Insiden Siber dengan otoritas, lembaga, dan/atau Penyelenggara lain.

(6) Rencana pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan memperhatikan sasaran waktu pemulihan dan sasaran titik pemulihan, paling sedikit mencakup:
   a. prosedur pemulihan untuk setiap kategori Insiden Siber;
   b. daftar personel pihak internal atau pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam pemulihan Insiden Siber; dan
   c. daftar sistem aplikasi termasuk aplikasi pendukung, infrastruktur teknologi informasi, dan sumber daya lain yang diperlukan dalam pemulihan Insiden Siber.

Pasal 42

(1) Penyusunan rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 40 huruf a menjadi bagian dari rencana keberlangsungan bisnis Penyelenggara.
(2) Rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) ditetapkan oleh manajemen tertinggi Penyelenggara.

Pasal 43

(1) Untuk melaksanakan penanganan dan pemulihan Insiden Siber, Penyelenggara menetapkan tim tanggap Insiden Siber dan kriteria pengaktifan tim tanggap Insiden Siber di level organisasi.
(2) Struktur dan susunan keanggotaan tim tanggap Insiden Siber di level organisasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan memperhatikan:
   a. kejelasan peran dan tanggung jawab;
   b. kapasitas dan kapabilitas anggota dalam melakukan penanganan dan pemulihan Insiden Siber; dan

c. keterlibatan personel lintas departemen, unit kerja, dan bagian, yang paling sedikit meliputi fungsi manajemen KKS, manajemen risiko, hukum, dan komunikasi.

(3) Struktur dan susunan keanggotaan tim tanggap Insiden Siber di level organisasi sebagaimana dimaksud pada ayat (1) dilaporkan kepada Bank Indonesia untuk koordinasi penanganan dan pemulihan Insiden Siber.

Paragraf 2
Pelaksanaan Simulasi dan Uji Coba
Penanganan dan Pemulihan Insiden Siber

Pasal 44

(1) Pelaksanaan simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 40 huruf b dilakukan dengan mengacu pada:
   a. profil Risiko Siber; dan
   b. kritikalitas fungsi bisnis dan Sistem Informasi.

(2) Pelaksanaan simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan skenario simulasi Serangan Siber sesuai tren perkembangan Siber.

(3) Simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) dilaksanakan dengan memastikan kelancaran operasional dan/atau layanan bisnis yang mempergunakan sistem aplikasi dan infrastruktur teknologi informasi Penyelenggara.

(4) Simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) dapat dilakukan dengan melibatkan:
   a. pihak ketiga; dan/atau
   b. pemangku kepentingan terkait.

(5) Simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Paragraf 3
Penanganan Insiden Siber

Pasal 45

(1) Penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 40 huruf c dilaksanakan berdasarkan rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 41 ayat (1).

(2) Penanganan Insiden Siber sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit dengan:
   a. mengaktifkan tim tanggap Insiden Siber di level organisasi;
   b. menyampaikan:
      1. notifikasi awal Insiden Siber paling lama 1 (satu) jam setelah Insiden Siber diketahui oleh Penyelenggara; dan
      2. laporan Insiden Siber paling lama 3 (tiga) hari kalender setelah Insiden Siber terjadi,

   kepada Bank Indonesia;

c. melakukan pendalaman Insiden Siber yang mencakup sumber, jenis, dan waktu serangan, analisis dampak, serta forensik terhadap Insiden Siber;
d. melakukan mitigasi Insiden Siber dan pembatasan dampak;
e. melaksanakan eskalasi dan penanganan Insiden Siber sesuai dengan tingkat dampak Insiden Siber; dan
f. melaksanakan penanganan Insiden Siber dengan menggunakan sumber daya internal dan/atau eksternal.

(3) Notifikasi awal Insiden Siber sebagaimana dimaksud pada ayat (2) huruf b angka 1 paling sedikit memuat informasi kontak pelapor, informasi umum Insiden Siber, dan asesmen awal dampak Insiden Siber.

(4) Laporan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf b angka 2 paling sedikit memuat informasi kontak pelapor, informasi umum Insiden Siber, analisis komprehensif dampak Insiden Siber, forensik Insiden Siber, kesimpulan, dan tindak lanjut perbaikan.

(5) Pendalaman Insiden Siber sebagaimana dimaksud pada ayat (2) huruf c dilakukan dengan:
a. memastikan catatan aktivitas Siber tercatat dan terjaga integritasnya saat Insiden Siber terjadi;
b. melakukan analisis dampak bisnis dan dampak teknis yang disebabkan Insiden Siber; dan
c. melakukan analisis terhadap akar permasalahan Insiden Siber.

(6) Mitigasi Insiden Siber dan pembatasan dampak sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan:
a. memastikan sumber Insiden Siber telah dihilangkan;
b. melakukan isolasi dampak Insiden Siber; dan
c. melakukan koordinasi penanganan isolasi dampak Insiden Siber dengan otoritas, lembaga, dan/atau Penyelenggara lain.

(7) Eskalasi dan penanganan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf e dapat mengaktifkan manajemen keberlangsungan bisnis Penyelenggara.

(8) Dalam melakukan eskalasi dan penanganan Insiden Siber sebagaimana dimaksud pada ayat (7), Penyelenggara dapat berkoordinasi dengan tim tanggap Insiden Siber sektor keuangan.

(9) Penanganan Insiden Siber sebagaimana dimaksud pada ayat (2) dapat menggunakan sumber daya eksternal dengan memastikan kerahasiaan informasi penanganan Insiden Siber terjaga.

Paragraf 4
Pelaksanaan Komunikasi Tindakan Penanganan Insiden Siber

Pasal 46

(1) Pelaksanaan komunikasi tindakan penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 40 huruf d dilakukan paling sedikit dengan:

a. menyusun strategi dan metode komunikasi penanganan dan pemulihan Insiden Siber;
b. mengomunikasikan penanganan Insiden Siber kepada pemangku kepentingan berdasarkan strategi dan metode komunikasi sebagaimana dimaksud dalam huruf a; dan
c. mengomunikasikan kemajuan penanganan Insiden Siber kepada Bank Indonesia.

(2) Strategi dan metode komunikasi sebagaimana dimaksud pada ayat (1) huruf a disusun dengan memperhatikan:
a. cakupan informasi;
b. waktu yang tepat;
c. penerima informasi atau pemangku kepentingan; dan
d. jalur atau kanal komunikasi.

(3) Komunikasi penanganan Insiden Siber kepada pemangku kepentingan sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan memperhatikan prinsip:
a. berorientasi pada pihak yang berkepentingan yang ditargetkan secara spesifik;
b. berkelanjutan dan konsisten;
c. waktu yang tepat; dan
d. kehati-hatian.

(4) Penyelenggara mengomunikasikan kemajuan penanganan Insiden Siber kepada Bank Indonesia sebagaimana dimaksud pada ayat (1) huruf c dengan menyampaikan progres penanganan Insiden Siber paling sedikit 1 (satu) kali dalam 1 (satu) hari.

Bagian Kedua
Pemulihan

Pasal 47

Pemulihan dilakukan paling sedikit dengan:
a. pengembalian layanan sebagaimana kondisi normal;
b. perbaikan berkelanjutan; dan
c. pelaksanaan komunikasi pemulihan Insiden Siber.

Paragraf 1
Pengembalian Layanan Sebagaimana Kondisi Normal

Pasal 48

(1) Dalam melakukan pengembalian layanan sebagaimana kondisi normal sebagaimana dimaksud dalam Pasal 47 huruf a, Penyelenggara menetapkan:
a. lokasi kerja alternatif;
b. pusat data yang terpisah; dan/atau
c. jaringan komunikasi data alternatif.

(2) Pengembalian layanan sebagaimana kondisi normal sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan:
a. hasil analisis dampak bisnis dan dampak teknis yang disebabkan Insiden Siber sebagaimana dimaksud dalam Pasal 45 ayat (5) huruf b;
b. rencana pemulihan Insiden Siber; dan
c. kritikalitas fungsi bisnis.

(3) Pengembalian layanan sebagaimana kondisi normal sebagaimana dimaksud pada ayat (1) dilakukan dengan:
   a. menyusun prioritisasi pemulihan;
   b. memastikan integritas *backup* dan infrastruktur teknologi informasi lainnya telah diverifikasi sebelum digunakan untuk pemulihan;
   c. memastikan keberhasilan pemulihan layanan berdasarkan kriteria yang telah ditetapkan Penyelenggara; dan
   d. menyusun laporan pemulihan Insiden Siber.

Paragraf 2
Perbaikan Berkelanjutan

Pasal 49

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 47 huruf b dilakukan paling sedikit dengan:
   a. melakukan evaluasi efektivitas dan perbaikan rencana penanganan dan pemulihan Insiden Siber atas dasar penanganan dan pemulihan Insiden Siber yang telah dilakukan; dan
   b. melakukan upaya penguatan KKS untuk memitigasi risiko Insiden Siber serupa.
(2) Upaya penguatan KKS sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan:
   a. memastikan akar permasalahan Insiden Siber diketahui untuk mencegah terulangnya kejadian serupa; dan
   b. mendapatkan *lesson learned*.

Paragraf 3
Pelaksanaan Komunikasi Pemulihan Insiden Siber

Pasal 50

(1) Pelaksanaan komunikasi pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 47 huruf c dilakukan paling sedikit dengan:
   a. mengomunikasikan pemulihan Insiden Siber kepada pemangku kepentingan berdasarkan strategi dan metode komunikasi pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 46 ayat (1) huruf a; dan
   b. mengomunikasikan kemajuan pemulihan Insiden Siber kepada Bank Indonesia.
(2) Komunikasi pemulihan Insiden Siber kepada pemangku kepentingan sebagaimana dimaksud pada ayat (1) huruf a dilakukan dengan memperhatikan prinsip:
   a. berorientasi pada pihak yang berkepentingan yang ditargetkan secara spesifik;
   b. berkelanjutan dan konsisten;
   c. waktu yang tepat; dan
   d. kehati-hatian.
(3) Penyelenggara mengomunikasikan kemajuan pemulihan Insiden Siber kepada Bank Indonesia sebagaimana dimaksud pada ayat (1) huruf b dengan menyampaikan progres pemulihan Insiden Siber.

Paragraf 4
Evaluasi Penanganan

Pasal 51

(1) Dalam melaksanakan respons sebagaimana dimaksud dalam Pasal 40 dan pemulihan sebagaimana dimaksud dalam Pasal 47, dilakukan evaluasi penanganan.
(2) Evaluasi penanganan sebagaimana dimaksud pada ayat (1) dilakukan untuk:
    a. mengukur efektivitas kegiatan penanganan; dan
    b. mendukung peningkatan kegiatan penanganan secara berkelanjutan.
(3) Evaluasi penanganan sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan:
    a. profil Risiko Siber;
    b. tren perkembangan Siber;
    c. hasil respons Insiden Siber; dan/atau
    d. hasil pemulihan Insiden Siber.
(4) Hasil evaluasi penanganan sebagaimana dimaksud pada ayat (1) disampaikan kepada manajemen tertinggi Penyelenggara.

BAB VI
PENYAMPAIAN DATA DAN INFORMASI

Pasal 52

(1) Penyelenggara menyampaikan data dan/atau informasi kepada Bank Indonesia.
(2) Data dan/atau informasi sebagaimana dimaksud pada ayat (1) terkait penerapan KKS meliputi area:
    a. tata kelola;
    b. pencegahan; dan
    c. penanganan.
(3) Data dan/atau informasi sebagaimana dimaksud pada ayat (2) disampaikan dalam bentuk dokumen, data mentah, dan/atau data olahan.
(4) Data dan/atau informasi sebagaimana dimaksud pada ayat (3) disampaikan melalui pelaporan secara:
    a. tahunan, meliputi:
        1. tingkat kematangan KKS; dan
        2. hasil identifikasi infrastruktur informasi vital, dan
    b. insidental pada saat terjadi Insiden Siber.

Pasal 53

(1) Laporan sebagaimana dimaksud dalam Pasal 52 ayat (4) disusun dan disampaikan secara lengkap, akurat, kini, utuh, dan tepat waktu.
(2) Laporan sebagaimana dimaksud pada ayat (1) disampaikan dengan lampiran bukti pendukung.
(3) Penyampaian laporan sebagaimana dimaksud pada ayat (1) dilakukan secara terpusat oleh setiap Penyelenggara.
(4) Penyampaian laporan tahunan sebagaimana dimaksud dalam Pasal 52 ayat (4) huruf a disampaikan paling lambat 31 Januari untuk periode pelaporan tahun sebelumnya.

(5) Dalam hal batas penyampaian laporan tahunan sebagaimana dimaksud pada ayat (4) bukan merupakan hari kerja operasional Bank Indonesia, laporan disampaikan pada hari kerja operasional Bank Indonesia sebelumnya.
(6) Dalam hal diperlukan, Bank Indonesia sewaktu-waktu dapat meminta Penyelenggara untuk menyampaikan laporan tingkat kematangan KKS terkini.

Pasal 54

(1) Bank Indonesia menetapkan infrastruktur informasi vital berdasarkan paling sedikit meliputi:
    a. ukuran;
    b. keterhubungan;
    c. ketergantian; dan
    d. kompleksitas.
(2) Penetapan infrastruktur informasi vital sebagaimana dimaksud pada ayat (1) dilakukan dengan mempertimbangkan hasil identifikasi sebagaimana dimaksud dalam Pasal 52 ayat 4 huruf a angka 2.

Pasal 55

(1) Penyelenggara menyampaikan laporan sebagaimana dimaksud dalam Pasal 52 ayat (4) kepada Bank Indonesia secara daring melalui sistem pelaporan Bank Indonesia.
(2) Penyampaian laporan secara daring sebagaimana dimaksud pada ayat (1) mengacu pada pedoman penyampaian laporan secara daring melalui sistem pelaporan Bank Indonesia.
(3) Pedoman penyampaian laporan secara daring sebagaimana dimaksud pada ayat (2) disampaikan Bank Indonesia kepada Penyelenggara melalui laman Bank Indonesia dan/atau media lain yang ditetapkan Bank Indonesia.
(4) Dalam hal sistem pelaporan sebagaimana dimaksud pada ayat (1) belum tersedia, laporan sebagaimana dimaksud dalam Pasal 52 ayat (4) disampaikan secara luring.

BAB VII
TATA CARA PENGENAAN SANKSI

Pasal 56

(1) Penyelenggara yang melanggar ketentuan dalam Peraturan Bank Indonesia mengenai KKS bagi penyelenggara Sistem Pembayaran, pelaku Pasar Uang dan Pasar Valuta Asing, serta pihak lain yang diatur dan diawasi Bank Indonesia, dikenai sanksi administratif berupa:
    a. teguran;
    b. kewajiban membayar;
    c. penghentian sementara, sebagian, atau seluruh kegiatan termasuk pelaksanaan kerja sama; dan/atau
    d. pencabutan izin dan/atau persetujuan yang telah diberikan.

(2) Pengenaan sanksi adminsitratif berupa teguran sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui penyampaian surat teguran tertulis.
(3) Pengenaan sanksi adminsitratif berupa kewajiban membayar sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan cara pendebitan rekening giro Penyelenggara pada Bank Indonesia bagi Penyelenggara yang memiliki rekening giro di Bank Indonesia.
(4) Pengenaan sanksi adminsitratif berupa kewajiban membayar sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan cara pembayaran kepada Bank Indonesia bagi Penyelenggara yang tidak memiliki rekening giro di Bank Indonesia.
(5) Pengenaan sanksi adminsitratif berupa penghentian sementara, sebagian, atau seluruh kegiatan termasuk pelaksanaan kerja sama sebagaimana dimaksud pada ayat (1) huruf c dilakukan Bank Indonesia dengan menyampaikan surat penghentian kegiatan usaha.
(6) Pengenaan sanksi adminsitratif berupa pencabutan izin dan/atau persetujuan yang telah diberikan sebagaimana dimaksud pada ayat (1) huruf d dilakukan Bank Indonesia dengan menyampaikan surat pencabutan izin dan/atau persetujuan.
(7) Sanksi administratif berupa kewajiban membayar sebagaimana dimaksud pada ayat (3) dan ayat (4) dikenakan paling banyak Rp5.000.000,00 (lima juta rupiah) per laporan.

BAB VIII
KOLABORASI

Bagian Kesatu
Pertukaran Informasi

Pasal 57
(1) Penyelenggara melakukan pertukaran informasi dengan memperhatikan klasifikasi informasi.
(2) Pertukaran informasi sebagaimana dimaksud pada ayat (1) dilakukan dengan menggunakan sarana berbagi yang dapat dibentuk oleh Bank Indonesia.

Bagian Kedua
Pencegahan Insiden Siber dan Efek Penularan

Pasal 58
(1) Dalam mencegah Insiden Siber dan efek penularan, Bank Indonesia dapat:
    a. mengisolasi akses terhadap infrastruktur Bank Indonesia; dan
    b. melakukan kolaborasi dan koordinasi dengan otoritas, lembaga, dan/atau Penyelenggara lain dalam penanganan Insiden Siber pada Penyelenggara.
(2) Bank Indonesia dapat mengisolasi akses Penyelenggara terhadap infrastruktur Bank Indonesia sebagaimana dimaksud pada ayat (1) huruf a jika:

a. terjadi Insiden Siber pada sistem yang digunakan oleh Penyelenggara yang terhubung dengan infrastruktur Bank Indonesia atau pada sistem lainnya yang berada di segmentasi jaringan yang sama; dan/atau
b. Insiden Siber yang terjadi berpotensi meluas.

(3) Penyelenggara dapat mengajukan pembukaan akses terhadap infrastruktur Bank Indonesia setelah melakukan penanganan dan pemulihan Insiden Siber serta layanan telah berjalan normal.

(4) Penyelenggara dapat melakukan isolasi akses terhadap infrastruktur Penyelenggara lain jika terjadi Insiden Siber pada sistem Penyelenggara lain yang terhubung secara langsung dan diyakini Insiden Siber yang terjadi berpotensi meluas.

Bagian Keempat
Kerja Sama dengan SRO

Pasal 59

(1) Bank Indonesia dapat menugaskan SRO untuk menyusun dan menetapkan prosedur KKS yang bersifat teknis dan spesifik.

(2) SRO dalam menetapkan prosedur KKS sebagaimana dimaksud pada ayat (1) harus mendapat persetujuan Bank Indonesia.

(3) Bank Indonesia dapat menunjuk SRO sebagai narahubung dengan Penyelenggara.

Pasal 60

(1) SRO yang dapat ditugaskan Bank Indonesia sebagaimana dimaksud dalam Pasal 59 ayat (1) merupakan SRO yang telah ditetapkan sebagaimana diatur dalam ketentuan Bank Indonesia mengenai Sistem Pembayaran dan ketentuan Bank Indonesia mengenai Pasar Uang dan Pasar Valuta Asing.

(2) Penetapan prosedur KKS sebagaimana dimaksud dalam Pasal 59 ayat (2) untuk mendukung:
a. penyelenggaraan Sistem Pembayaran mengacu pada penerbitan ketentuan SRO sebagaimana diatur dalam ketentuan Bank Indonesia mengenai Sistem Pembayaran; dan
b. pengembangan Pasar Uang dan Pasar Valuta Asing mengacu pada penerbitan ketentuan SRO sebagaimana diatur dalam ketentuan Bank Indonesia mengenai Pasar Uang dan Pasar Valuta Asing.

Pasal 61

SRO yang ditunjuk Bank Indonesia sebagai narahubung dengan Penyelenggara sebagaimana dimaksud dalam Pasal 59 ayat (3) melakukan koordinasi:

a. penyusunan usulan skenario simulasi Serangan Siber sektor keuangan yang dilakukan dengan:
1. meminta SRO untuk melakukan presentasi dengan melibatkan anggota SRO yang mempunyai kompetensi yang baik terkait penyusunan simulasi Serangan Siber;

2. berperan aktif bersama Bank Indonesia, SRO lain, dan/atau otoritas lainnya dalam membahas penyusunan simulasi Serangan Siber;
3. berperan aktif dalam mencari solusi atas simulasi Serangan Siber sebagai mitigasi risiko Serangan Siber; dan
4. menerapkan solusi sebagaimana dimaksud pada angka 3 terhadap anggota SRO dalam hal terjadi Serangan Siber;

b. pelaksanaan sosialisasi terkait ketentuan KKS Bank Indonesia dan/atau prosedur KKS oleh SRO dengan:
1. melibatkan seluruh anggota SRO untuk berperan aktif dalam kegiatan sosialisasi;
2. menyampaikan masukan dari anggota SRO terkait penerapan KKS; dan
3. menyampaikan usulan solusi terkait permasalahan KKS yang dihadapi oleh anggota SRO; dan

c. kegiatan lainnya yang ditetapkan Bank Indonesia.

Pasal 62

Bank Indonesia menentukan batas waktu penugasan SRO sebagaimana dimaksud dalam Pasal 59.

BAB IX
PENERAPAN KKS

Pasal 63

(1) Dalam hal Penyelenggara memiliki layanan digitalisasi yang terhubung secara langsung dengan:
a. sistem aplikasi dan/atau infrastruktur teknologi informasi Bank Indonesia; dan/atau
b. sistem aplikasi dan/atau infrastruktur teknologi informasi Penyelenggara lain,
ketentuan penerapan KKS sebagaimana diatur dalam Peraturan Anggota Dewan Gubernur ini berlaku sepenuhnya.

(2) Dalam hal Penyelenggara menggunakan:
a. sistem aplikasi dan/atau infrastruktur teknologi informasi pihak lain (*client*); atau
b. sistem aplikasi dan/atau infrastruktur teknologi informasi sendiri yang tidak terhubung secara langsung dengan sistem aplikasi dan/atau infrastruktur teknologi informasi Bank Indonesia dan/atau Penyelenggara lain,
ketentuan penerapan KKS sebagaimana diatur dalam Peraturan Anggota Dewan Gubernur ini hanya berlaku untuk pengaturan tertentu.

(3) Dalam hal Penyelenggara menggunakan:
a. *end user device* atau perangkat *stand-alone* lainnya; dan/atau
b. perangkat analog,
ketentuan penerapan KKS sebagaimana diatur dalam Peraturan Anggota Dewan Gubernur ini tidak berlaku.

Pasal 64

Pengaturan tertentu sebagaimana dimaksud dalam Pasal 63 ayat (2) meliputi:

a. pengamanan data, sistem aplikasi, dan infrastruktur teknologi informasi sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf a;
b. penetapan kebijakan KKS oleh manajemen tertinggi Penyelenggara sebagaimana dimaksud dalam Pasal 7 ayat (3);
c. penerapan dan komunikasi kebijakan, standar, dan prosedur KKS kepada seluruh pihak internal dan/atau pihak ketiga terkait sebagaimana dimaksud dalam Pasal 7 ayat (5);
d. penerapan manajemen KKS sebagaimana dimaksud dalam Pasal 9 ayat (1);
e. pengukuran tingkat kematangan KKS sebagaimana dimaksud dalam Pasal 10 ayat (2);
f. pelaksanaan audit KKS secara berkala sebagaimana dimaksud dalam Pasal 12 ayat (1);
g. pelaksanaan program peningkatan budaya KKS kesadaran (*awareness*) sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf a;
h. pemberian program peningkatan budaya KKS kepada pihak internal sebagaimana dimaksud dalam Pasal 13 ayat (3) huruf a;
i. pelaksanan penginian profil Risiko Siber sebagaimana dimaksud dalam Pasal 14 ayat (3);
j. identifikasi Risiko Siber sebagaimana dimaksud dalam Pasal 15 ayat (1);
k. dokumentasi hasil identifikasi Risiko Siber pada inventaris risiko (*risk register*) sebagaimana dimaksud dalam Pasal 15 ayat (5);
l. kemananan pihak internal dan pihak ketiga yang dipastikan dengan memeriksa latar belakang personel pihak internal dan/atau pihak ketiga yang akan dipekerjakan sebagaimana dimaksud dalam Pasal 21 ayat (1) huruf a serta mewajibkan penandatanganan perjanjian atau surat pernyataan kerahasiaan data dan/atau informasi sebagaimana dimaksud dalam Pasal 21 ayat (1) huruf c;
m. manajemen akses logis dan fisik terhadap sistem aplikasi dan infrastruktur teknologi informasi sebagaimana dimaksud dalam Pasal 22 huruf a dan pelindungan yang memadai terhadap KKS dalam perjanjian kerja sama antara Penyelenggara dengan pihak ketiga sebagaimana dimaksud dalam Pasal 22 huruf d;
n. implementasi konfigurasi pengamanan berupa metode otentikasi dan otorisasi sesuai profil Risiko Siber sebagaimana dimaksud dalam Pasal 23 huruf e;
o. pengamanan dan pengendalian data dan/atau informasi dengan memastikan kepatuhan pelindungan data pribadi sesuai dengan ketentuan peraturan perundang-undangan sebagaimana dimaksud dalam Pasal 24 ayat (1) huruf b;
p. pemantauan akses fisik dan logis dengan menerapkan sistem deteksi paling sedikit pada area dan/atau objek kritikal atau vital sebagaimana dimaksud dalam Pasal 27

huruf b dan memastikan setiap perubahan terhadap akses logis dan fisik serta konfigurasi dikelola melalui manajemen perubahan sebagaimana dimaksud dalam Pasal 27 huruf d;

q. Pemindaian Kerentanan Siber terhadap sistem aplikasi, infrastruktur teknologi informasi, dan data Penyelenggara sebagaimana dimaksud dalam Pasal 29 ayat (1);
r. pembaruan sistem pemantauan segera setelah versi perangkat lunak terkini dirilis dan telah teruji sebagaimana dimaksud dalam Pasal 39 ayat (2);
s. penyusunan rencana respons Insiden Siber paling sedikit mencakup daftar personel pihak internal atau pihak ketiga berikut peran, tanggung jawab, dan kontak yang dapat dihubungi dalam penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 41 ayat (4) huruf b;
t. penanganan Insiden Siber dilaksanakan berdasarkan rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 45 ayat (1);
u. penanganan insiden siber dilaksanakan paling sedikit dengan menyampaikan notifikasi awal Insiden Siber dan laporan Insiden Siber sebagaimana dimaksud dalam Pasal 45 ayat (2) huruf b;
v. mitigasi Insiden Siber dan pembatasan dampak dengan memastikan sumber Insiden Siber telah dihilangkan sebagaimana dimaksud dalam Pasal 45 ayat (6) huruf a;
w. perbaikan berkelanjutan dengan melakukan evaluasi efektivitas dan perbaikan rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 49 ayat (1) huruf a;
x. penyampaian data dan informasi sebagaimana dimaksud dalam Pasal 52 sampai dengan Pasal 55;
y. tata cara pengenaan sanksi sebagaimana dimaksud dalam Pasal 56; dan
z. kolaborasi sebagaimana dimaksud dalam Pasal 57 sampai dengan Pasal 62.

BAB X
KETENTUAN LAIN-LAIN

Pasal 65

Pelaporan tahunan sebagaimana dimaksud dalam Pasal 53 ayat (4) pertama kali disampaikan kepada Bank Indonesia pada Januari 2026 untuk periode laporan tahun 2025.

BAB XI
KETENTUAN PENUTUP

Pasal 66

Peraturan Anggota Dewan Gubernur ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 31 Desember 2024

ANGGOTA DEWAN GUBERNUR,

TTD

JUDA AGUNG

PENJELASAN
ATAS
PERATURAN ANGGOTA DEWAN GUBERNUR
NOMOR 24 TAHUN 2024
TENTANG
KEAMANAN SISTEM INFORMASI DAN KETAHANAN SIBER BAGI PENYELENGGARA SISTEM PEMBAYARAN, PELAKU PASAR UANG DAN PASAR VALUTA ASING, SERTA PIHAK LAIN YANG DIATUR DAN DIAWASI BANK INDONESIA

I. UMUM

Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan memperkuat kewenangan Bank Indonesia dalam melakukan pengaturan dan pengawasan kepada pelaku usaha sektor keuangan dan penyelenggaraan inovasi teknologi sektor keuangan khususnya terkait penerapan keamanan dan keandalan Sistem Informasi termasuk ketahanan Siber.

Penguatan kewenangan tersebut sejalan dengan upaya Bank Indonesia untuk mendukung percepatan pembagunan ekonomi keuangan digital yang berkelanjutan sebagaimana dimuat dalam *Blueprint* Sistem Pembayaran Indonesia 2025. Peningkatan digitalisasi pada sektor keuangan tidak hanya membantu pertumbuhan ekonomi keuangan digital yang berkelanjutan, namun juga menimbulkan dampak lain berupa peningkatan eksposur Risiko Siber. Insiden Siber yang terjadi pada sektor keuangan dapat menimbulkan kerugian keuangan dan mengganggu stabilitas Sistem Keuangan.

Sebagai upaya mitigasi Risiko Siber, Bank Indonesia melakukan pengaturan dan pengawasan KKS bagi Penyelenggara Sistem Pembayaran, pelaku Pasar Uang dan Pasar Valuta Asing, serta pihak lain yang diatur dan diawasi oleh Bank Indonesia. Hal ini dilakukan agar Penyelenggara tersebut dapat membangun KKS, antara lain dengan melaksanakan kegiatan antisipatif, adaptif, dan proaktif terhadap Risiko Siber. Selain itu, diperlukan upaya penguatan pengawasan dan kolaborasi dalam pencegahan serta penanganan Insiden Siber yang berdampak secara sistemik maupun nonsistemik bagi Sistem Keuangan.

Berdasarkan hal tersebut, Bank Indonesia telah menerbitkan Peraturan Bank Indonesia tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia.

II. PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2

Huruf a

Cakupan PJP mengacu pada Peraturan Bank Indonesia mengenai Sistem Pembayaran dan Peraturan Bank Indonesia mengenai PJP.

Huruf b

Cakupan PIP mengacu pada Peraturan Bank Indonesia mengenai Sistem Pembayaran dan Peraturan Bank Indonesia mengenai PIP.

Huruf c

Cakupan PUSK PUVA mengacu pada Peraturan Bank Indonesia mengenai Pasar Uang dan Pasar Valuta Asing.

Huruf d

Cakupan Lembaga Pendukung Pasar Uang mengacu pada Peraturan Bank Indonesia mengenai Pasar Uang dan Pasar Valuta Asing.

Huruf e

Cakupan Lembaga Pendukung Pasar Valuta Asing mengacu pada Peraturan Bank Indonesia mengenai Pasar Uang dan Pasar Valuta Asing.

Huruf f

Cakupan Penyelenggara Kegiatan Usaha Penukaran Valuta Asing Bukan Bank mengacu pada Peraturan Bank Indonesia mengenai kegiatan usaha penukaran valuta asing bukan bank.

Huruf g

Cukup jelas.

Pasal 3

Cukup jelas.

Pasal 4

Cukup jelas.

Pasal 5

Cukup jelas.

Pasal 6

Ayat (1)

Manajemen tertinggi antara lain direksi atau pimpinan manajemen tertinggi lainnya yang berwenang dan bertanggung jawab penuh atas pengurusan organisasi.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 7

Ayat (1)

Pihak ketiga antara lain vendor di bidang layanan Sistem Informasi, tenaga kerja perjanjian kerja waktu tertentu, tenaga kerja alih daya (*outsourcing*), dan konsultan eksternal.

Ayat (2)

Cukup jelas.

Ayat (3)

Lihat penjelasan Pasal 6 ayat (1).

Ayat (4)

Cukup jelas.

Ayat (5)

Yang dimaksud dengan “pihak internal” adalah pihak yang dipekerjakan oleh Penyelenggara untuk waktu tidak tertentu.

Lihat penjelasan ayat (1).

Ayat (6)

Cukup jelas.

Pasal 8

Cukup jelas.

Pasal 9

Cukup jelas.

Pasal 10

Cukup jelas.

Pasal 11

Cukup jelas.

Pasal 12

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang dimaksud dengan “otoritas lain” adalah otoritas di sektor keuangan dan lembaga nasional yang bergerak di bidang KKS antara lain OJK dan BSSN.

Ayat (4)

Cukup jelas.

Pasal 13

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Program peningkatan budaya KKS berupa kesadaran (*awareness*):

1. bertujuan untuk memberikan pemahaman kepada individu mengenai hal yang perlu diketahui, antara lain informasi yang penting untuk diwaspadai atau dipahami;
2. dilakukan dengan metode pengajaran yang menggunakan media seperti video, buletin, poster, atau materi singkat lainnya; dan
3. disampaikan kepada pihak internal, pihak ketiga, dan/atau konsumen.

Huruf b

Program peningkatan budaya KKS berupa pelatihan:

1. bertujuan untuk mengajarkan cara melakukan sesuatu, dengan fokus pada pengembangan keterampilan;

2. dilakukan dengan metode pengajaran praktis, antara lain studi kasus dan praktik langsung; dan
3. disampaikan kepada pihak internal dan/atau pihak ketiga.

Huruf c

Program peningkatan budaya KKS berupa edukasi:

1. bertujuan untuk memberikan pengetahuan yang mendalam tentang alasan di balik suatu tindakan sehingga individu dapat memahami latar belakang atau dasar dari suatu konsep;
2. dilakukan dengan metode pengajaran teoritis, antara lain seminar dan klasikal; dan
3. disampaikan kepada pihak internal.

Ayat (3)

Huruf a

Lihat penjelasan Pasal 7 ayat (5).

Huruf b

Lihat penjelasan Pasal 7 ayat (1).

Huruf c

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Ayat (6)

Cukup jelas.

Pasal 14

Cukup jelas.

Pasal 15

Cukup jelas.

Pasal 16

Cukup jelas.

Pasal 17

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Yang dimaksud dengan "*maximum tolerable period of disruption*" adalah jangka waktu maksimal dimana dampak terhentinya tugas kritikal dapat diterima Penyelenggara.

Huruf c

Cukup jelas.

Ayat (3)

Huruf a

Sasaran waktu pemulihan (*recovery time objective*) merupakan jangka waktu yang diperlukan untuk memulihkan sistem aplikasi, infrastruktur teknologi informasi, dan/atau layanan kritikal yang dapat diterima Penyelenggara setelah terjadi Insiden Siber.

Sasaran titik pemulihan (*recovery point objective*) merupakan waktu maksimal kehilangan data yang bisa ditoleransi setelah terjadi Insiden Siber.

Huruf b

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 18

Cukup jelas.

Pasal 19

Cukup jelas.

Pasal 20

Cukup jelas.

Pasal 21

Ayat (1)

Pihak ketiga lihat penjelasan Pasal 7 ayat (1).

Pihak internal lihat penjelasan Pasal 7 ayat (5).

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 22

Huruf a

Akses logis (*logical access*) antara lain nama akun (*username*) dan kata sandi (*password*), token otentikasi, dan jaringan komunikasi data.

Akses fisik *(physical access)* antara lain kunci dan kartu akses, biometrik, dan kamera keamanan.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Yang dimaksud dengan "dokumentasi" adalah dokumentasi terhadap tujuan, proses pengembangan, dan data yang digunakan dalam model kecerdasan artifisial.

Pasal 23

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Secure coding pada pengembangan sistem aplikasi bertujuan untuk antara lain mengurangi risiko terungkapnya kerahasiaan informasi dan potensi risiko dampak lainnya.

Huruf d

Cukup jelas.

Huruf e

Metode otentikasi berupa otentikasi satu faktor, otentikasi dua faktor, otentikasi multifaktor.
Contoh otentikasi satu faktor yaitu kata sandi (*password).*
Contoh otentikasi dua faktor yaitu kata sandi *password* dan token.
Contoh otentikasi multifaktor yaitu kata sandi *(password)*, token, dan biometrik.

Huruf f

Pertahanan terhadap *adversarial attack* bertujuan untuk melindungi model kecerdasan artifisial dari manipulasi input yang dapat mengganggu prediksi atau fungsi model kecerdasan artifisial, yang berdampak terhadap keandalan dan integritas informasi.

Pasal 24

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Pengamanan data dan/atau informasi pada saat disimpan termasuk melakukan *backup*.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Pasal 25

Ayat (1)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Kode jahat (*malicious code*) merupakan perangkat lunak termasuk program komputer atau *script* yang dibuat dan dikirim dengan tujuan untuk merusak sistem aplikasi dan/atau infrastruktur teknologi informasi.
Kode jahat (*malicious code*) antara lain kode untuk mencuri data, merusak *file,* menonaktifkan sistem, atau menyebarkan *malware.*
Kode tidak sah (*unauthorized code)* merupakan perangkat lunak termasuk program komputer atau *script* yang diinstal pada sistem aplikasi dan/atau infrastruktur teknologi informasi tanpa izin atau otorisasi dari Penyelenggara.

Huruf e

Cukup jelas.

Ayat (2)

Deteksi yang dilaksanakan secara terpusat antara lain menggunakan mekanisme *security operation center.*

Mekanisme *security operation center* antara lain meliputi kegiatan *red-teaming*, *blue-teaming*, dan *threat hunting*.

Ayat (3)

Cukup jelas.

Pasal 26

Huruf a

Lihat penjelasan Pasal 22 huruf a.

Huruf b

Cukup jelas.

Huruf c

Pemindaian Kerentanan Siber antara lain:

a. uji penetrasi (*penetration test*) yang merupakan pengujian dengan menggunakan sistem Penyelenggara dan bertujuan untuk menerobos sistem pengamanan yang ada, sesuai dengan batasan yang telah ditentukan sebelumnya; dan
b. asesmen kerentanan (*vulnerability assessment*) yang merupakan asesmen untuk mendapatkan Kerentanan Siber pada sistem Penyelenggara.

Pasal 27

Lihat penjelasan Pasal 22 huruf a.

Pasal 28

Cukup jelas.

Pasal 29

Cukup jelas.

Pasal 30

Cukup jelas.

Pasal 31

Cukup jelas.

Pasal 32

Cukup jelas.

Pasal 33

Cukup jelas.

Pasal 34

Ayat (1)

Huruf a

Asal Serangan Siber antara lain dari internal dan/atau eksternal Penyelenggara.

Profil *threat actor* antara lain berupa individu, kelompok, dan/atau, negara.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)
Cukup jelas.
Ayat (4)
Cukup jelas.

Pasal 35
Lihat penjelasan Pasal 25 ayat (1) huruf d.

Pasal 36
Cukup jelas.

Pasal 37
Cukup jelas.

Pasal 38
Cukup jelas.

Pasal 39
Cukup jelas.

Pasal 40
Cukup jelas.

Pasal 41
Ayat (1)
Huruf a
Cukup jelas.
Huruf b
Cukup jelas.
Huruf c
Cukup jelas.
Huruf d
Lihat penjelasan Pasal 17 ayat (3) huruf a.
Ayat (2)
Cukup jelas.
Ayat (3)
Cukup jelas.
Ayat (4)
Huruf a
Analisis *post-mortem* antara lain proses evaluasi yang dilakukan setelah terjadinya Insiden Siber untuk memahami penyebab Insiden Siber, mengidentifikasi Kerentanan Siber, dan menentukan langkah-langkah perbaikan guna mencegah Insiden Siber terulang di masa depan.
Huruf b
Cukup jelas.
Huruf c
Cukup jelas.
Ayat (5)
Cukup jelas.
Ayat (6)
Cukup jelas.

Pasal 42
Cukup jelas.

Pasal 43
Cukup jelas.

Pasal 44
Cukup jelas.

Pasal 45
Cukup jelas.

Pasal 46
Cukup jelas.

Pasal 47
Cukup jelas.

Pasal 48
Cukup jelas.

Pasal 49
Cukup jelas.

Pasal 50
Cukup jelas.

Pasal 51
Cukup jelas.

Pasal 52
Cukup jelas.

Pasal 53
Ayat (1)
Cukup jelas.
Ayat (2)
Lampiran bukti pendukung antara lain laporan audit KKS secara berkala dan laporan uji penetrasi (*penetration test)*.
Ayat (3)
Cukup jelas.
Ayat (4)
Cukup jelas.
Ayat (5)
Cukup jelas.
Ayat (6)
Cukup jelas.

Pasal 54
Ayat (1)
Huruf a
Yang dimaksud dengan “ukuran” adalah tingkat eksposur Penyelenggara yang diukur berdasarkan frekuensi, volume transaksi, dan jumlah pengguna Sistem Informasi.
Huruf b
Yang dimaksud dengan “keterhubungan” adalah keterhubungan antar-Sistem Informasi yang dipergunakan dalam pelaksanaan kegiatan usaha Penyelenggara di Sistem Keuangan dan perekonomian nasional.

Huruf c

Yang dimaksud dengan ”ketergantian” adalah ketersediaan Sistem Informasi alternatif yang dapat dipergunakan untuk bertransaksi.

Huruf d

Yang dimaksud dengan ”kompleksitas” adalah variasi dan ketergantungan komponen Sistem Informasi.

Ayat (2)

Cukup jelas.

Pasal 55

Cukup jelas.

Pasal 56

Cukup jelas.

Pasal 57

Ayat (1)

Cukup jelas.

Ayat (2)

Sarana berbagi antara lain surat elektronik, aplikasi, laman, dan/atau sarana lainnya.

Pasal 58

Cukup jelas.

Pasal 59

Cukup jelas.

Pasal 60

Cukup jelas.

Pasal 61

Cukup jelas.

Pasal 62

Cukup jelas.

Pasal 63

Ayat (1)

Layanan digitalisasi yang terhubung secara langsung antara lain *application programming interface* dan *host-to-host*.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Yang dimaksud dengan “*end user device*” adalah perangkat teknologi yang digunakan langsung oleh pengguna akhir (*end user*) untuk mengakses, mengelola, atau berinteraksi dengan data, aplikasi, atau layanan dalam suatu sistem.

End user device antara lain *notebook*, *PC desktop*, media tablet, dan *smartphone*.

Huruf b

Cukup jelas.

Pasal 64

Cukup jelas.

Pasal 65

Cukup jelas.

Pasal 66

Cukup jelas.