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

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR BANK INDONESIA,

Menimbang : a. bahwa dalam mewujudkan tujuan Bank Indonesia untuk mencapai stabilitas nilai rupiah, memelihara stabilitas sistem pembayaran, dan turut menjaga stabilitas sistem keuangan dalam rangka mendukung pertumbuhan ekonomi yang berkelanjutan, diperlukan pemanfaatan teknologi informasi untuk mendorong percepatan pembangunan ekonomi keuangan digital;

b. bahwa pemanfaatan teknologi informasi berpotensi meningkatkan eksposur risiko siber yang dapat menimbulkan kerugian keuangan dan mengganggu stabilitas sistem keuangan, sehingga perlu dibangun keamanan sistem informasi dan ketahanan siber yang mengacu pada standar internasional dan praktik terbaik;

c. bahwa untuk membangun keamanan sistem informasi dan ketahanan siber, diperlukan pengaturan 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;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan 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;

Mengingat : 1. Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 66, Tambahan Lembaran Negara Republik Indonesia Nomor 3843) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Republik Indonesia Tahun

2023 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6845);

2. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6845);

MEMUTUSKAN:

Menetapkan : 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.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bank Indonesia 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
KERANGKA PENGATURAN DAN PENGAWASAN KKS

Pasal 2

Bank Indonesia melakukan pengaturan dan pengawasan KKS dengan tujuan menciptakan KKS pada Penyelenggara dalam mendukung tujuan Bank Indonesia.

Pasal 3

Sasaran pengaturan dan pengawasan KKS meliputi:
a. peningkatan KKS Penyelenggara untuk mencegah dan menangani dampak Serangan Siber;
b. peningkatan manajemen Risiko Siber Penyelenggara; dan
c. penguatan pengawasan dan kolaborasi dalam pencegahan Insiden Siber dan/atau penanganan Insiden Siber yang terjadi pada Penyelenggara.

Pasal 4

Prinsip dasar pelaksanaan KKS meliputi:
a. kejelasan peran dan tanggung jawab;
b. strategi yang komprehensif;
c. manajemen Risiko Siber terintegrasi dengan *enterprise risk management*;
d. integrasi dengan budaya KKS; dan
e. kesiapan menghadapi Insiden Siber.

Pasal 5

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 6

Ruang lingkup pengaturan dan pengawasan KKS meliputi:
a. tata kelola;
b. pencegahan;
c. penanganan;
d. pengawasan; dan
e. kolaborasi.

BAB III
TATA KELOLA

Bagian Kesatu
Umum

Pasal 7

Tata kelola sebagaimana dimaksud dalam Pasal 6 huruf a meliputi:
a. strategi dan kebijakan KKS; dan
b. budaya KKS.

Bagian Kedua
Strategi dan Kebijakan KKS

Pasal 8

(1) Strategi dan kebijakan KKS sebagaimana dimaksud dalam Pasal 7 huruf a 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 9

(1) Rencana strategis KKS sebagaimana dimaksud dalam Pasal 8 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) Penyelenggara melakukan evaluasi secara berkala terhadap rencana strategis KKS sebagaimana dimaksud pada ayat (1) sesuai dengan perkembangan Risiko Siber.
(3) Ketentuan lebih lanjut mengenai rencana strategis KKS sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Paragraf 2
Kebijakan, Standar, dan Prosedur KKS

Pasal 10

(1) Kebijakan, standar, dan prosedur KKS sebagaimana dimaksud dalam Pasal 8 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) Penyelenggara melakukan evaluasi secara berkala terhadap kebijakan, standar, dan prosedur KKS

sebagaimana dimaksud pada ayat (1) untuk memastikan kecukupan dan efektivitas kebijakan, standar, dan prosedur KKS sesuai perkembangan terkini.

(3) Ketentuan lebih lanjut mengenai kebijakan, standar, dan prosedur KKS sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Paragraf 3
Fungsi Organisasi KKS

Pasal 11

Fungsi organisasi KKS sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf c meliputi:
a. manajemen KKS;
b. manajemen Risiko Siber; dan
c. audit KKS.

Pasal 12

(1) Dalam menjalankan fungsi organisasi KKS sebagaimana dimaksud dalam Pasal 11, Penyelenggara memperhatikan:
   a. efektivitas dan efisiensi;
   b. akuntabilitas; dan
   c. kapasitas dan kapabilitas sumber daya manusia.
(2) Dalam menjalankan fungsi organisasi KKS sebagaimana dimaksud pada ayat (1), Penyelenggara dapat bekerja sama dengan pihak lain.

Pasal 13

(1) Penyelenggara menerapkan manajemen KKS sebagaimana dimaksud dalam Pasal 11 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 bertanggung jawab pada manajemen tertinggi dalam implementasi aktivitas KKS.
(3) Dalam penerapan manajemen KKS sebagaimana dimaksud pada ayat (1), manajemen KKS dapat bekerja sama dengan pihak lain.

Pasal 14

(1) Penyelenggara menerapkan manajemen Risiko Siber sebagaimana dimaksud dalam Pasal 11 huruf b sesuai praktik terbaik.
(2) Manajemen Risiko Siber sebagaimana dimaksud pada ayat (1) mencakup aspek pelindungan terhadap:
   a. kerahasiaan;
   b. integritas; dan
   c. ketersediaan,

   informasi dalam mendukung kelangsungan proses bisnis.

Pasal 15

(1) Penyelenggara menerapkan manajemen Risiko Siber sebagaimana dimaksud dalam Pasal 14 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 secara berkala.
(2) Ketentuan lebih lanjut mengenai pengukuran tingkat kematangan KKS sebagaimana dimaksud pada ayat (1) huruf c diatur dalam Peraturan Anggota Dewan Gubernur.

Pasal 16

(1) Penyelenggara melaksanakan audit KKS sebagaimana dimaksud dalam Pasal 11 huruf c sebagai sarana untuk memastikan kepatuhan terhadap regulasi, kebijakan, standar, dan prosedur, serta efektivitas pengendalian dalam implementasi KKS.
(2) Audit KKS sebagaimana dimaksud pada ayat (1) paling sedikit mencakup:
   a. tata kelola;
   b. pencegahan; dan
   c. penanganan.

Pasal 17

(1) Penyelenggara melakukan audit KKS sebagaimana dimaksud dalam Pasal 16 secara berkala.
(2) Pelaksanaan audit KKS sebagaimana dimaksud pada ayat (1) dilakukan oleh pihak internal dan/atau pihak eksternal secara independen.
(3) Ketentuan lebih lanjut mengenai pelaksanaan audit KKS sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Bagian Ketiga
Budaya KKS

Pasal 18

(1) Budaya KKS sebagaimana dimaksud dalam Pasal 7 huruf b diterapkan sebagai sarana untuk meningkatkan kesadaran Risiko Siber serta perilaku positif dan etika Siber.
(2) Budaya KKS sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Penyelenggara melalui program peningkatan budaya KKS.
(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) dilaksanakan secara berkala dengan melibatkan manajemen tertinggi sebagai teladan.

Pasal 19

Ketentuan lebih lanjut mengenai budaya KKS sebagaimana dimaksud dalam Pasal 18 diatur dalam Peraturan Anggota Dewan Gubernur.

BAB IV
PENCEGAHAN

Bagian Kesatu
Umum

Pasal 20

(1) Pencegahan sebagaimana dimaksud dalam Pasal 6 huruf b meliputi:
    a. identifikasi;
    b. proteksi; dan
    c. deteksi.
(2) Pencegahan sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Penyelenggara untuk mengantisipasi Insiden Siber.

Bagian Kedua
Identifikasi

Pasal 21

(1) Identifikasi sebagaimana dimaksud dalam Pasal 20 ayat (1) huruf a 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) Identifikasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Penyelenggara untuk memahami profil Risiko Siber guna memperoleh gambaran menyeluruh terkait Risiko Siber yang dihadapi serta prioritisasi pengendalian yang dibutuhkan.
(4) Ketentuan lebih lanjut mengenai identifikasi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Paragraf 1
Identifikasi Risiko Siber

Pasal 22

(1) Identifikasi Risiko Siber sebagaimana dimaksud dalam Pasal 21 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) Informasi Kerentanan Siber dan Ancaman Siber sebagaimana dimaksud pada ayat (1) huruf a dapat

bersumber dari sarana pertukaran informasi yang dibentuk Bank Indonesia atau sarana informasi lain.

Paragraf 2
Asesmen Risiko Siber

Pasal 23

Asesmen Risiko Siber sebagaimana dimaksud dalam Pasal 21 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 prioritasi mitigasi terhadap Kerentanan Siber dan Ancaman Siber mulai dari yang paling tinggi sampai dengan yang paling rendah.

Paragraf 3
Analisis Dampak Bisnis

Pasal 24

Analisis dampak bisnis sebagaimana dimaksud dalam Pasal 21 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 prioritasi pengendalian risiko; dan
c. menganalisis Sistem Informasi kritikal yang berdampak luas terhadap stabilitas Sistem Keuangan.

Pasal 25

Sistem Informasi kritikal yang berdampak luas sebagaimana dimaksud dalam Pasal 24 huruf c dikategorikan sebagai infrastruktur informasi vital.

Bagian Ketiga
Proteksi

Pasal 26

(1) Proteksi sebagaimana dimaksud dalam Pasal 20 ayat (1) huruf b meliputi:
    a. pembangunan sistem pertahanan; dan
    b. pengamanan dan pelindungan data dan/atau informasi.
(2) Proteksi sebagaimana dimaksud pada ayat (1) dilakukan oleh Penyelenggara untuk membangun sistem pertahanan yang dapat mencegah terjadinya Serangan Siber berdasarkan profil risiko serta mengamankan data dan/atau informasi pada setiap tahapan siklus pengelolaan data dan/atau informasi.

Paragraf 1
Pembangunan Sistem Pertahanan

Pasal 27

Pembangunan sistem pertahanan sebagaimana dimaksud dalam Pasal 26 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.

Paragraf 2
Pengamanan dan Pelindungan Data dan Informasi

Pasal 28

Pengamanan dan pelindungan data dan/atau informasi sebagaimana dimaksud dalam Pasal 26 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.

Bagian Keempat
Deteksi

Pasal 29

(1) Deteksi sebagaimana dimaksud dalam Pasal 20 ayat (1) huruf c 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 oleh Penyelenggara untuk:
    a. mengetahui Kerentanan Siber, Serangan Siber, dan/atau Insiden Siber yang terjadi;
    b. memberikan peringatan dini; dan
    c. melakukan penguatan KKS secara berkelanjutan.

Paragraf 1
Pemantauan

Pasal 30

Pemantauan sebagaimana dimaksud dalam Pasal 29 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.

Paragraf 2
Analisis Hasil Pemantauan

Pasal 31

Analisis hasil pemantauan sebagaimana dimaksud dalam Pasal 29 ayat (1) huruf b dilakukan paling sedikit dengan:
a. menganalisis catatan aktivitas Siber; dan
b. menganalisis Kerentanan Siber dan potensi Serangan Siber.

Paragraf 3
Analisis Serangan Siber

Pasal 32

Analisis Serangan Siber sebagaimana dimaksud dalam Pasal 29 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.

Paragraf 4
Analisis Kode Jahat atau Kode Tidak Sah

Pasal 33

Analisis kode jahat atau kode tidak sah sebagaimana dimaksud dalam Pasal 29 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.

Paragraf 5
Pemeliharaan dan Pengujian Sistem Deteksi

Pasal 34

(1) Pemeliharaan dan pengujian sistem deteksi sebagaimana dimaksud dalam Pasal 29 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) Ketentuan lebih lanjut mengenai pemeliharaan dan pengujian sistem deteksi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

BAB V
PENANGANAN

Bagian Kesatu
Umum

Pasal 35

(1) Penanganan sebagaimana dimaksud dalam Pasal 6 huruf c meliputi:
   a. respons; dan
   b. pemulihan.
(2) Penanganan sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Penyelenggara untuk:
   a. memitigasi Insiden Siber; dan
   b. mengembalikan layanan sebagaimana kondisi normal.

Bagian Kedua
Respons

Pasal 36

(1) Respons sebagaimana dimaksud dalam Pasal 35 ayat (1) huruf a 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.
(2) Respons sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Penyelenggara untuk:
   a. mempersiapkan proses penanganan Insiden Siber;
   b. mencegah perluasan dampak Insiden Siber; dan
   c. melakukan komunikasi penanganan Insiden Siber.

Paragraf 1
Penyusunan Rencana Penanganan dan
Pemulihan Insiden Siber

Pasal 37

(1) Penyusunan rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 36 ayat (1) 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) Rencana penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) disusun oleh Penyelenggara sebagai bagian dari rencana keberlangsungan bisnis Penyelenggara.
(3) Penyelenggara membentuk tim tanggap Insiden Siber di level organisasi yang berperan dalam penanganan Insiden Siber.

(4) Tim tanggap Insiden Siber sebagaimana dimaksud pada ayat (3) dapat melibatkan personel lintas departemen, unit kerja, dan bagian.

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

Pasal 38

(1) Pelaksanaan simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 36 ayat (1) huruf b dilakukan secara komprehensif dan berkala.
(2) Simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) dapat dilakukan dengan melibatkan pihak lain.
(3) Ketentuan lebih lanjut mengenai simulasi dan uji coba penanganan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Pasal 39

Penyelenggara melakukan evaluasi efektivitas dan perbaikan rencana penanganan dan pemulihan Insiden Siber atas dasar hasil simulasi dan uji coba penanganan dan pemulihan Insiden Siber.

Paragraf 3
Penanganan Insiden Siber

Pasal 40

Penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 36 ayat (1) huruf c 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.

Paragraf 4
Pelaksanaan Komunikasi Tindakan Penanganan Insiden Siber

Pasal 41

Pelaksanaan komunikasi tindakan penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 36 ayat (1) 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.

Bagian Ketiga
Pemulihan

Pasal 42

(1) Pemulihan sebagaimana dimaksud dalam Pasal 35 ayat (1) huruf b dilakukan paling sedikit dengan:
    a. pengembalian layanan sebagaimana kondisi normal;
    b. perbaikan berkelanjutan; dan
    c. pelaksanaan komunikasi pemulihan Insiden Siber.
(2) Pemulihan sebagaimana dimaksud pada ayat (1) dilakukan oleh Penyelenggara untuk:
    a. mengembalikan layanan sebagaimana kondisi normal sesuai prioritas; dan
    b. penguatan KKS agar Insiden Siber tidak terulang kembali.

Paragraf 1
Pengembalian Layanan Sebagaimana Kondisi Normal

Pasal 43

(1) Dalam melakukan pengembalian layanan sebagaimana kondisi normal sebagaimana dimaksud dalam Pasal 42 ayat (1) huruf a, Penyelenggara menetapkan:
    a. lokasi kerja alternatif;
    b. pusat data yang terpisah; dan/atau
    c. jaringan komunikasi data alternatif,
    sesuai hasil analisis dampak penanganan Insiden Siber.
(2) Pengembalian layanan sebagaimana kondisi normal sebagaimana dimaksud pada ayat (1) sesuai dengan rencana pemulihan Insiden Siber dan mengacu pada prioritas pemulihan.

Paragraf 2
Perbaikan Berkelanjutan

Pasal 44

Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 42 ayat (1) 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.

Paragraf 3
Pelaksanaan Komunikasi Pemulihan Insiden Siber

Pasal 45

Pelaksanaan komunikasi pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 42 ayat (1) huruf c dilakukan paling sedikit dengan:

a. mengomunikasikan pemulihan Insiden Siber kepada pemangku kepentingan mengacu pada strategi dan metode komunikasi sebagaimana dimaksud dalam Pasal 41 huruf a; dan
b. mengomunikasikan kemajuan pemulihan Insiden Siber kepada Bank Indonesia.

BAB VI
PENGAWASAN

Bagian Kesatu
Umum

Pasal 46

Pengawasan sebagaimana dimaksud dalam Pasal 6 huruf d meliputi:

a. mekanisme pengawasan; dan
b. penyampaian data dan/atau informasi.

Bagian Kedua
Mekanisme Pengawasan

Pasal 47

Bank Indonesia melakukan pengawasan untuk memastikan tercapainya KKS pada Penyelenggara.

Pasal 48

Bank Indonesia melakukan pengawasan terhadap Penyelenggara dengan menggunakan pendekatan pengawasan berbasis risiko dan/atau kepatuhan.

Pasal 49

Mekanisme pengawasan terhadap Penyelenggara dilakukan melalui:

a. pengawasan tidak langsung; dan
b. pengawasan langsung.

Pasal 50

(1) Pengawasan tidak langsung sebagaimana dimaksud dalam Pasal 49 huruf a dilakukan melalui pemantauan, identifikasi, dan/atau asesmen terhadap laporan, data dan/atau informasi yang disampaikan oleh Penyelenggara kepada Bank Indonesia.

(2) Pengawasan tidak langsung sebagaimana dimaksud pada ayat (1) dapat dilakukan secara terintegrasi termasuk terhadap perusahaan induk, perusahaan anak, dan/atau pihak terafiliasi lain.

Pasal 51

(1) Mekanisme pengawasan langsung sebagaimana dimaksud dalam Pasal 49 huruf b dilakukan melalui tatap muka atau mekanisme lain yang ditetapkan oleh Bank Indonesia.
(2) Pengawasan langsung sebagaimana dimaksud pada ayat (1) dapat dilakukan secara terintegrasi termasuk terhadap perusahaan induk, perusahaan anak, dan/atau pihak terafiliasi lain.
(3) Objek pengawasan langsung sebagaimana dimaksud pada ayat (1) meliputi dokumen, infrastruktur, Sistem Informasi, dan objek lain yang digunakan oleh Penyelenggara.
(4) Periode pengawasan langsung sebagaimana dimaksud pada ayat (1) dilakukan secara berkala dan/atau sewaktu-waktu.
(5) Dalam melakukan pengawasan langsung, Bank Indonesia dapat menugaskan pihak lain untuk dan atas nama Bank Indonesia.

Pasal 52

Berdasarkan hasil pengawasan tidak langsung sebagaimana dimaksud dalam Pasal 50 dan pengawasan langsung sebagaimana dimaksud dalam Pasal 51, Bank Indonesia melakukan tindak lanjut pengawasan berupa meminta Penyelenggara untuk:

a. melakukan atau tidak melakukan sesuatu; dan/atau
b. membatasi kegiatan dan/atau layanan Penyelenggara.

Pasal 53

Bank Indonesia dapat berkoordinasi dengan otoritas lain jika perusahaan induk Penyelenggara, perusahaan anak Penyelenggara, dan/atau pihak terafiliasi lain berada di bawah pengawasan otoritas lain.

Bagian Ketiga
Penyampaian Data dan Informasi

Pasal 54

(1) Penyelenggara menyampaikan data dan/atau informasi sebagaimana dimaksud dalam Pasal 46 huruf b 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.

(5) Ketentuan lebih lanjut mengenai tata cara penyampaian data dan/atau informasi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

Pasal 55

(1) Laporan sebagaimana dimaksud dalam Pasal 54 ayat (4) wajib disampaikan oleh Penyelenggara kepada Bank Indonesia.

(2) Penyelenggara yang melanggar ketentuan sebagaimana dimaksud pada ayat (1) 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.

(3) Sanksi administratif berupa kewajiban membayar sebagaimana dimaksud pada ayat (2) huruf b, dikenakan paling banyak Rp5.000.000,00 (lima juta rupiah) per laporan.

(4) Ketentuan lebih lanjut mengenai tata cara penyampaian laporan dan pengenaan sanksi administratif diatur dalam Peraturan Anggota Dewan Gubernur.

BAB VII
KOLABORASI

Bagian Kesatu
Umum

Pasal 56

(1) Kolaborasi sebagaimana dimaksud dalam Pasal 6 huruf e meliputi:
   a. pertukaran informasi;
   b. pencegahan Insiden Siber dan efek penularan; dan
   c. kerja sama dengan SRO.

(2) Bank Indonesia melakukan kolaborasi sebagaimana dimaksud pada ayat (1) untuk:
   a. memperkuat kerja sama dengan Penyelenggara dan/atau asosiasi Penyelenggara; dan
   b. memperkuat KKS dalam pencegahan dan penanganan Insiden Siber.

Bagian Kedua
Pertukaran Informasi

Pasal 57

(1) Penyelenggara melakukan pertukaran informasi sebagaimana dimaksud dalam Pasal 56 ayat (1) huruf a terkait hasil identifikasi Kerentanan Siber, Ancaman Siber, Serangan Siber, dan Insiden Siber yang dapat mengganggu stabilitas Sistem Keuangan ke Bank Indonesia.
(2) Informasi hasil identifikasi yang dipertukarkan sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:
    a. sumber dan pola Ancaman Siber dan Serangan Siber;
    b. celah keamanan yang berdampak pada Kerentanan Siber; dan
    c. pembelajaran dari cara penanganan Insiden Siber.
(3) Bank Indonesia dapat meneruskan informasi hasil identifikasi Kerentanan Siber, Ancaman Siber, Serangan Siber, dan Insiden Siber sebagaimana dimaksud pada ayat (1) kepada otoritas terkait dan/atau Penyelenggara lain.

Pasal 58

Bank Indonesia dapat membentuk sarana berbagi sebagai sarana pertukaran informasi Kerentanan Siber, Ancaman Siber, Serangan Siber, dan Insiden Siber antar-Penyelenggara.

Bagian Ketiga
Pencegahan Insiden Siber dan Efek Penularan

Pasal 59

Dalam mencegah Insiden Siber dan efek penularan sebagaimana dimaksud dalam Pasal 56 ayat (1) huruf b, 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.

Pasal 60

Bank Indonesia dapat berkolaborasi dan berkoordinasi dengan otoritas, lembaga, dan/atau Penyelenggara untuk memastikan kesiapan penanganan Insiden Siber.

Bagian Keempat
Kerja Sama dengan SRO

Pasal 61

(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.

(4) Ketentuan lebih lanjut mengenai mekanisme pengajuan permohonan persetujuan atas prosedur KKS diatur dalam Peraturan Anggota Dewan Gubernur.

BAB VIII
PENERAPAN KKS

Pasal 62

(1) Penyelenggara melakukan penerapan KKS sesuai dengan klasifikasi Penyelenggara.
(2) Klasifikasi Penyelenggara sebagaimana dimaksud pada ayat (1) untuk:
    a. PJP mengacu pada Peraturan Bank Indonesia mengenai Sistem Pembayaran dan Peraturan Bank Indonesia mengenai PJP;
    b. PIP mengacu pada Peraturan Bank Indonesia mengenai Sistem Pembayaran dan Peraturan Bank Indonesia mengenai PIP;
    c. PUSK PUVA, Lembaga Pendukung Pasar Uang, dan Lembaga Pendukung Pasar Valuta Asing dilakukan berdasarkan tingkatan risiko infrastruktur pasar keuangan yang mengacu pada Peraturan Bank Indonesia mengenai Pasar Uang dan Pasar Valuta Asing; dan
    d. Penyelenggara selain Penyelenggara sebagaimana dimaksud dalam huruf a sampai dengan huruf c dilakukan dengan mempertimbangkan tingkatan risiko infrastruktur teknologi informasi dan/atau berdasarkan tingkatan risiko yang ditetapkan oleh Bank Indonesia.
(3) Ketentuan lebih lanjut mengenai penerapan KKS sesuai dengan klasifikasi Penyelenggara sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Anggota Dewan Gubernur.

BAB IX
KETENTUAN PENUTUP

Pasal 63

Peraturan Bank Indonesia ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bank Indonesia ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 18 April 2024

GUBERNUR BANK INDONESIA,

BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA

PERRY WARJIYO

Diundangkan di Jakarta
pada tanggal 22 April 2024

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

#KUMHAMPASTI
Ditandatangani secara elektronik oleh :

YASONNA H. LAOLY

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2024 NOMOR 9/BI

PENJELASAN
ATAS
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

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 perlu menetapkan 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

Cukup jelas.

Pasal 3

Cukup jelas.

Pasal 4

Huruf a

Yang dimaksud dengan "kejelasan peran dan tanggung jawab" adalah kejelasan peran dan tanggung jawab Penyelenggara untuk memastikan KKS telah dikelola secara efektif.

Huruf b

Yang dimaksud dengan "strategi yang komprehensif" adalah mengimplementasikan strategi KKS secara menyeluruh.

Huruf c

Yang dimaksud dengan "manajemen Risiko Siber terintegrasi dengan *enterprise risk management*" adalah mengintegrasikan KKS dalam manajemen risiko sehingga meningkatkan keefektifan pengendalian terhadap Ancaman Siber yang dinamis.

Huruf d

Yang dimaksud dengan "integrasi dengan budaya KKS" adalah menginternalisasikan program budaya sadar KKS melalui peningkatan kompetensi dan sosialisasi secara berkala.

Huruf e

Yang dimaksud dengan "kesiapan menghadapi Insiden Siber" adalah mengantisipasi kemungkinkan terjadinya Insiden Siber serta menjalankan pemulihan Insiden Siber secara efektif.

Pasal 5

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 6

Cukup jelas.

Pasal 7

Cukup jelas.

Pasal 8

Cukup jelas.

Pasal 9

Cukup jelas.

Pasal 10

Ayat (1)

Huruf a

Cukup jelas.

Huruf b

Pihak ketiga antara lain vendor di bidang layanan Sistem Informasi.

Huruf c

Yang dimaksud dengan "manajemen *fraud*" adalah pengelolaan terhadap kecurangan atau penipuan yang diakibatkan oleh Kerentanan Siber.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 11

Cukup jelas.

Pasal 12

Ayat (1)

Cukup jelas.

Ayat (2)

Kerja sama dengan pihak lain dilakukan antara lain dengan pihak yang memiliki kompetensi di bidang audit, manajemen Risiko Siber, dan bidang lainnya yang mendukung pelaksanaan KKS.

Pasal 13

Ayat (1)

Cukup jelas.

Ayat (2)

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

Ayat (3)

Lihat penjelasan Pasal 12 ayat (2).

Pasal 14

Cukup jelas.

Pasal 15
Cukup jelas.

Pasal 16
Cukup jelas.

Pasal 17
Cukup jelas.

Pasal 18
Ayat (1)
Perilaku positif dalam membangun budaya KKS antara lain menjaga kerahasiaan data dan informasi, serta melakukan akses informasi secara aman melalui laman resmi.
Etika Siber dalam membangun budaya KKS antara lain menghindari pelanggaran hak kekayaan intelektual dalam kegiatan Siber, serta mencegah pemanfaatan media Siber sebagai sarana penyebaran informasi palsu.
Ayat (2)
Cukup jelas.
Ayat (3)
Huruf a
Cukup jelas.
Huruf b
Lihat penjelasan Pasal 10 ayat (1) huruf b.
Huruf c
Cukup jelas.
Ayat (4)
Lihat penjelasan Pasal 13 ayat (2).

Pasal 19
Cukup jelas.

Pasal 20
Cukup jelas.

Pasal 21
Cukup jelas.

Pasal 22
Ayat (1)
Cukup jelas.
Ayat (2)
Sarana informasi lain antara lain penyedia atau komunitas berbagi informasi intelijen Siber.

Pasal 23
Cukup jelas.

Pasal 24
Cukup jelas.

Pasal 25
Cukup jelas.

Pasal 26

Cukup jelas.

Pasal 27

Huruf a

Yang dimaksud dengan "memastikan keamanan pihak internal dan pihak ketiga pada setiap tahapan siklus kerja" adalah memastikan pihak internal dan pihak ketiga memiliki antara lain kompetensi, integritas, dan etika Siber, sebelum, selama, dan setelah dipekerjakan oleh Penyelenggara.

Huruf b

Cukup jelas.

Huruf c

Implementasi konfigurasi pengamanan terhadap Sistem Informasi yang digunakan antara lain:

1. pengendalian akses logis dan fisik *(logical and physical access)*;
2. penginian versi perangkat lunak *(update patch)*;
3. pelindungan perangkat yang berpotensi menjadi titik masuk Kerentanan Siber (*endpoint security*); dan
4. segmentasi jaringan.

Segmentasi jaringan antara lain jaringan internet, jaringan intranet, dan jaringan ekstranet.

Pasal 28

Cukup jelas.

Pasal 29

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)

Cukup jelas.

Pasal 30

Huruf a

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

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

Huruf b

Aktivasi sistem peringatan dini dipicu jika indikator ambang batas terlampaui.

Huruf c

Pemindaian Kerentanan Siber antara lain 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.

Pasal 31

Huruf a

Aktivitas Siber dapat tercatat di dalam *log system* atau *event monitoring.*

Huruf b

Cukup jelas.

Pasal 32

Huruf a

Fraud terkait Siber merupakan kecurangan atau penipuan yang diakibatkan oleh Kerentanan Siber.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Pasal 33

Cukup jelas.

Pasal 34

Cukup jelas.

Pasal 35

Cukup jelas.

Pasal 36

Cukup jelas.

Pasal 37

Ayat (1)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

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.

Ayat (2)

Rencana keberlangsungan bisnis Penyelenggara *(business continuity plan)* merupakan kebijakan dan prosedur yang memuat rangkaian kegiatan yang terencana untuk menjamin keberlangsungan bisnis dan/atau layanan Penyelenggara ketika terjadi keadaan tidak normal dan/atau keadaan darurat.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 38

Cukup jelas.

Pasal 39

Cukup jelas.

Pasal 40

Cukup jelas.

Pasal 41

Huruf a

Cukup jelas.

Huruf b

Pemangku kepentingan antara lain pihak internal Penyelenggara, nasabah Penyelenggara, Bank Indonesia, Otoritas Jasa Keuangan, dan Badan Siber dan Sandi Negara.

Huruc c

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
Cukup jelas.

Pasal 54
Cukup jelas.

Pasal 55
Cukup jelas.

Pasal 56
Cukup jelas.

Pasal 57
Cukup jelas.

Pasal 58
Cukup jelas.

Pasal 59
Cukup jelas.

Pasal 60
Koordinasi Bank Indonesia dengan otoritas, lembaga, dan/atau Penyelenggara antara lain melakukan simulasi Serangan Siber sektor keuangan.

Pasal 61
Ayat (1)
Cukup jelas.
Ayat (2)
Cukup jelas.
Ayat (3)
SRO berperan aktif sebagai narahubung dengan Penyelenggara antara lain melakukan koordinasi penyusunan usulan skenario simulasi Serangan Siber sektor keuangan.
Ayat (4)
Cukup jelas.

Pasal 62
Cukup jelas.

Pasal 63

Cukup jelas.

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 77/BI